

Churer Schriften zur Informationswissenschaft

Herausgegeben von
Wolfgang Semar

Arbeitsbereich
Informationswissenschaft

Schrift 146

Mithilfe von Digital Nudging mehr Privatsphäre in sozialen Netzwerken?

Digital Nudging in sozialen Netzwerken

Jeffrey Santana de Jesus

Chur 2022

Churer Schriften zur Informationswissenschaft

Herausgegeben von Wolfgang Semar

Schrift 146

Mithilfe von Digital Nudging mehr Privatsphäre in sozialen Netzwerken?

Digital Nudging in sozialen Netzwerken

Jeffrey Santana de Jesus

Diese Publikation entstand im Rahmen einer Thesis zum Bachelor of Science FHGR in Digital Business Management.

Referent: Dr. Caroline Dalmus

Korreferentin: Prof. Armando Schär

Verlag: Fachhochschule Graubünden

ISSN: 1660-945X

Ort, Datum: Chur, Januar 2022

Abstract

Das Ziel dieser Arbeit besteht darin, herauszufinden, inwiefern Social-Norm-Digital-Nudges das Verhalten von Personen dazu lenken können, in sozialen Netzwerken weniger ihrer Daten preiszugeben beziehungsweise bewusster mit diesen umzugehen.

Um diese Frage zu beantworten, wurde eine experimentelle Umfrage unter 366 Teilnehmerinnen und Teilnehmern durchgeführt. Dabei erhielt ein Teil der Gruppe einen Social-Norm-Digital-Nudge.

Durch die experimentelle Befragung konnten Erkenntnisse zum Einsatz von Social-Norm-Digital-Nudges gewonnen werden, jedoch konnte kein signifikanter Unterschied zwischen der Gruppe mit Social-Norm-Digital-Nudge und derjenigen ohne festgestellt werden. In gewissen Altersgruppen war der Unterschied nur knapp nicht signifikant. Daher stellt diese Bachelorarbeit fest, dass gewisse nicht signifikante Unterschiede vorhanden sind, die unter Betrachtung der gewonnenen Erkenntnisse dieser Arbeit noch genauer untersucht werden sollten.

Inhaltsverzeichnis

1	Einleitung.....	1
1.1	Relevanz.....	2
1.2	Forschungsfrage, Zielsetzung und Methodik.....	3
1.3	Aufbau der Arbeit.....	3
2	Privatsphäre.....	5
2.1	Überblick.....	5
2.2	Risiken beim Teilen von persönlichen Inhalten.....	6
2.3	Einstellungen zum Schutz der Privatsphäre in sozialen Netzwerken.....	7
3	Selbstoffenbarung.....	13
3.1	Begriffsbestimmung.....	13
3.2	Online- versus Offline-Selbstoffenbarung.....	13
3.3	Umfang der Selbstoffenbarung in sozialen Netzwerken.....	14
3.4	Bedürfnis nach Popularität.....	15
3.5	Soziales Umfeld.....	15
3.6	Privacy Paradox.....	16
4	Nudging.....	19
4.1	Eingrenzung.....	19
4.2	Libertärer Paternalismus.....	19
4.3	Kritik.....	21
4.4	Digital Nudging.....	22
5	Soziale Normen.....	25
5.1	Überblick.....	25
5.2	Social-Norm-Nudge.....	25
6	Hypothesen.....	27
6.1	Ableitung.....	27
6.2	Operationalisierung.....	30
7	Methodik.....	35
7.1	Erhebungsdesign.....	35
7.2	Pretest und Stichprobenerhebung.....	37
7.3	Datenauswertung.....	38
8	Ergebnisse.....	41
8.1	Stichprobe.....	41
8.2	Wirkung des Nudges auf die Selbstoffenbarung (Hypothese 1).....	43
8.3	Einfluss des Risikobewusstseins (Hypothese H2a & H2b).....	45
8.4	Einfluss des Bedürfnisses nach Popularität (Hypothese H3a & H3b).....	46

8.5	Einfluss der Gruppenkonformität (Hypothese H4a & H4b).....	47
8.6	Berücksichtigung der demografischen Merkmale	48
8.6.1	Wirkung des Nudges auf die Selbstoffenbarung (Hypothese 1).....	48
8.6.2	Einfluss des Risikobewusstseins (Hypothese H2a & H2b)	53
8.6.3	Einfluss des Bedürfnisses nach Popularität (Hypothese H3a & H3b)	54
8.6.4	Einfluss der Gruppenkonformität (Hypothese H4a & H4b).....	56
8.7	Fazit der Resultate.....	56
9	Diskussion	59
9.1	Ergebnisdiskussion	59
9.2	Grenzen der Arbeit	62
10	Fazit.....	65
11	Literaturverzeichnis.....	67
12	Anhang	77
12.1	Anhang I.....	77
12.2	Anhang II.....	80
12.3	Anhang III.....	95

Abbildungsverzeichnis

Abbildung 1: Übersicht der Privatsphäre-Einstellungen von YouTube. Quelle: Google LLC, o.D.	8
Abbildung 2: Datenschutzeinstellungen für Minderjährige auf TikTok. Quelle: ByteDance Ltd., o.D.-a	11
Abbildung 3: Hypothesenmodell.....	30
Abbildung 4: Dimensionen und Attribute der Variablen «Selbstoffenbarung».....	31
Abbildung 5: Hypothesenmodell (nach der Auswertung).....	57

Tabellenverzeichnis

Tabelle 1: Items der Variablen «Risikobewusstsein».....	32
Tabelle 2: Items der Variablen «Bedürfnis nach Popularität»	33
Tabelle 3: Items der Variablen «Gruppenkonformität».....	34
Tabelle 4: Nudges im einfaktoriellen Forschungsdesign	37
Tabelle 5: Demografische Merkmale der Stichprobe der Experimental- und der Kontrollgruppe	43
Tabelle 6: Unterschiede in der Wahl der Teilen Option zwischen Experimental- und Kontrollgruppe	45
Tabelle 7: Resultat der Regression für die Hypothesen H2a & H2b.....	46
Tabelle 8: Resultat der Regression für die Hypothesen H3a & H3b.....	47
Tabelle 9: Resultat der Regression für die Hypothesen H4a & H4b.....	47
Tabelle 10: Unterschiede in der Wahl der Teilen Option zwischen Experimental- und Kontrollgruppe (ohne Alter 19–24).	50
Tabelle 11: Mittelwerte der Selbstoffenbarung im Vergleich zum Bildungsniveau.....	51
Tabelle 12: Mittelwerte der Selbstoffenbarung im Vergleich zur Erwerbstätigkeit.	52
Tabelle 13: Selbstoffenbarung im Vergleich zur Erfahrung mit Risiken.....	53
Tabelle 14: Resultat der Regression für die Hypothesen H2a & H2b unter Berücksichtigung des Alters.	54
Tabelle 15: Resultat der Regression für die Hypothesen H3a & H3b unter Berücksichtigung des Alters.	55
Tabelle 16: Resultat der Regression für die Hypothesen H4a & H4b unter Berücksichtigung des Alters.	56
Tabelle 17: Vollständige Auflistung aller Nudges im Experiment.....	79
Tabelle 18: Forscherversion des Fragebogens.	94

Abkürzungsverzeichnis

JAMES	Jugend Aktivitäten Medien – Erhebung Schweiz
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften
SPSS	Superior Performing Software System

1 Einleitung

Soziale Netzwerke sind heute ein Teil des Alltags von über 7.1 Millionen Schweizerinnen und Schweizern (We Are Social, Hootsuite & DataReportal, 2021, S. 17). Sie bieten die Möglichkeit, mit Bekannten in Kontakt zu bleiben oder sogar neue Freundschaften zu knüpfen. Einige finden sogar ihre Lebenspartnerin oder ihren Lebenspartner über soziale Netzwerke. Für die Nutzung der meisten Formen entstehen keine Kosten oder Abgebühren. Die Einnahmen gehen vielmehr aus der Werbung hervor, die eine Nutzerin oder ein Nutzer auf dem sozialen Netzwerk sehen. Soziale Netzwerke profitieren daher von der Anzahl der Nutzenden sowie ihrer Verweildauer auf ihnen (Falch, Henten, Tadayoni & Windekilde, 2009, S. 20–22). Um die Verweildauer und die Attraktivität eines Netzwerkes zu optimieren, sind geeignete Inhalte nötig, die durch seine Nutzenden generiert werden (Abramova, Wagner, Krasnova & Buxmann, 2017, S. 1). Die Daten, die durch die Nutzenden veröffentlicht werden, enthalten teilweise persönliche Informationen zu ihrer Person. Dadurch gehen auch Risiken aus der Nutzung von sozialen Netzwerken hervor.

Im März 2018 enthüllten verschiedene bekannte Zeitungen und ein britischer Fernsehsender die Cambridge-Analytica-Affäre des bekannten sozialen Netzwerks Facebook, das gleichzeitig auch in andere Datenschutzskandale involviert war (Betschon, 2018). Die Firma Cambridge Analytica arbeitete mit politischen Parteien in verschiedenen Ländern in einer Beraterfunktion zusammen, um Online-Kampagnen für deren Wahlen zu erstellen. Die Firma soll am Präsidentenwahlkampf von 2016 in den USA und an der Brexit-Abstimmung in Grossbritannien mitgewirkt haben. Die von der Beraterfirma genutzten Methoden waren rechtswidrig: Sie erstellte Wahlprofile von potenziellen Wahlberechtigten anhand Daten aus ihren Facebook-Profilen. Die Daten kamen von der Zustimmung zur Nutzung der Daten von Facebook, die die Teilnehmende im Rahmen einer angeblichen bezahlten akademischen Studie nebenbei erteilt hatten. Das Problem bestand darin, dass sie Cambridge Analytica auch die Zustimmung dazu erteilt hatten, auf die Daten ihrer Freunde zuzugreifen (Langer, 2018). Dieser Fall zeigt, wie persönliche Daten auch in anonymisierter Form von Institutionen missbraucht werden können. Es könnte angenommen werden, dass die Nutzerzahlen Facebooks in Folge des Skandals eingebrochen sind, doch konnten sich diese sogar im Zeitraum vom 2018 bis 2020 um 21% steigern (Facebook Inc., 2021). Personen scheinen Risiken, die sie nicht direkt betreffen und die ihnen somit keine direkten Schäden zufügen, somit zu unterschätzen. Dabei handelt es sich um eine sogenannte Optimismusverzerrung (optimism bias) (Kokolakis, 2017, S. 129).

Es bestehen nicht nur im Missbrauch von persönlichen Daten durch Institutionen Risiken, sondern Daten können auch von Personen missbraucht werden. Im Digitalzeitalter ist es für jeden einfach, Inhalte zu vervielfältigen und zu manipulieren. Dadurch kann selten sichergestellt werden, dass Daten beispielsweise nach ihrem Entfernen aus einem sozialen Netzwerk wirklich nicht mehr existieren (Rudin, 2003, S. 137–144). In der JAMES-Studie 2020 (Jugend Aktivitäten Medien – Erhebung Schweiz) konnte festgestellt werden, dass die Anzahl der Fälle zunimmt, in denen Jugendliche von fremden Personen mit unerwünschten sexuellen Absichten angesprochen werden. So gaben 55% der teilnehmenden Mädchen an, bereits einen solchen Kontakt gehabt zu haben (Bernath et al., 2020, S. 51–54). Diese Statistik zeigt, dass sich im Internet auch Personen mit negativen Absichten befinden. Daher ist es empfehlenswert, die eigenen persönlichen Daten gegenüber Dritten, aber auch gegenüber Bekannten zu schützen. Durch die Verwendung von Social-Norm-Digital-Nudges könnte das Verhalten in Bezug auf die Selbstoffenbarung von persönlichen Daten bewusster und sicherer gestaltet werden. Somit könnten Personen weiterhin soziale Netzwerke nutzen, ihre Daten hier aber bewusster preisgeben. Daraus ergibt sich die Frage, ob durch die Platzierung von Social-Norm-Digital-Nudges die Sicherheitssensibilität in Bezug auf die Selbstoffenbarung erhöht werden kann. Dies soll im Rahmen der vorliegenden Bachelorarbeit untersucht werden.

1.1 Relevanz

Nudging ist eine stark diskutierte Methode in der Verhaltensökonomie, die der Beeinflussung von Personen dient. Es wird in ihrem Rahmen versucht, mit leichten Veränderungen in der Entscheidungsarchitektur Personen so zu beeinflussen, dass sie für sich bessere Entscheidungen treffen (Thaler & Sunstein, 2009). Durch die Zunahme an digitalen Lösungen und damit auch Entscheidungen wird das Nudging immer wesentlicher im digitalen Bereich. Dank der Gestaltungsfreiheit in digitalen Interaktionsmöglichkeiten können vielseitige Nudges eingesetzt werden. Doch ist das Nudging hier nicht auf den Austausch am Bildschirm beschränkt, es entstehen auch neue Interaktionsmöglichkeiten – zum Beispiel Virtual Reality oder Augmented Reality – in deren Rahmen ebenfalls Entscheidungen getroffen und mit Nudges unterstützt werden können (Schär & Stanoevska-Slabeva, 2019, S. 2–3). Das Nudging im digitalen Bereich wird «Digital Nudging» genannt (Weinmann, Schneider & Brocke, 2016, S. 433–434).

Mit der Zunahme neuer Möglichkeiten gehen neue Risiken einher, auch in Bezug auf den Schutz der eigenen Daten. Das Privacy-Paradoxon gibt die Diskrepanz zwischen dem Selbstoffenbarungsverhalten und dem Risikobewusstsein zu erkennen: Personen mei-

nen, besorgt um den Schutz ihrer persönlichen Daten zu sein, geben diese aber trotzdem bei der Verwendung von sozialen Netzwerken preis (Young & Quan-Haase, 2013, S. 479). So möchten sie ihre Daten schützen, scheitern daran aber. Dies gilt, obwohl die Missbrauchsgefahr bei einfacher und kostenloser Vervielfältigung von Daten hoch ist (Rudin, 2003, S. 137–144). Das Konzept des Nudgings könnte sich im Bereich des Datenschutzes als effiziente Methode zur Verringerung des Privacy-Paradoxons erweisen. In der Untersuchung von Masaki et al. (2020) wurde ein möglicher Effekt des Social-Norm-Digital-Nudges entdeckt, er konnte aber nicht nachgewiesen werden. Durch ein Social-Norm-Digital-Nudge könnte somit in Zukunft Personen dabei geholfen werden, ihre persönlichen Daten besser zu schützen. Genauere Erkenntnisse über die Wirkung sowie die Gestaltung eines solchen Nudges sollen im Rahmen der vorliegenden Arbeit abgeleitet werden.

1.2 Forschungsfrage, Zielsetzung und Methodik

Inwiefern können Social-Norm-Digital Nudges das Verhalten von Personen dahingehend beeinflussen, dass sie weniger Daten bei der Verwendung von sozialen Netzwerken preisgeben?

Die oben genannte forschungsleitende Fragestellung möchte der Verfasser dieser Arbeit in ihrem Rahmen beantworten. Das Ziel dieser Arbeit besteht darin, herauszufinden, inwiefern Social-Norm-Digital-Nudges das Verhalten von Personen dazu lenken können, in sozialen Netzwerken weniger ihrer Daten preiszugeben beziehungsweise bewusster mit diesen umzugehen. In dieser Arbeit wird der Schutz der eigenen Daten vor Personen thematisiert, die sowohl bekannt als auch unbekannt sein können. Ihr Schutz gegenüber Institutionen wird in dieser Arbeit nicht untersucht, um den Rahmen dieser Arbeit nicht zu sprengen. Die Forschungsfrage soll anhand einer experimentellen Umfrage beantwortet werden, da mit diesem die Wirkung des Nudges gemessen werden kann. Im Rahmen der empirischen Untersuchung sollen die Probanden und die Probandinnen mit Nudges dazu verleitet werden, ihre Option beim Teilen gewisser Informationen niedriger zu wählen, als sie es ohne Nudge täten. Um die Privatsphäre der Teilnehmenden nicht selbst zu verletzen, wird keine Eingabe persönlicher Informationen (ausser dem Alter) verlangt, sondern nur hypothetisch mithilfe von Vignetten simuliert.

1.3 Aufbau der Arbeit

Diese Bachelorarbeit wurde in zehn Kapitel unterteilt. In den Kapiteln zwei bis fünf wird der Forschungsstand zu verschiedenen Themen (Privatsphäre, Selbstoffenbarung, Nud-

ging, soziale Normen) skizziert, der für die Aufstellung von Hypothesen in Kapitel sechs sowie deren Operationalisierung grundlegend ist. In Kapitel sieben wird auf die Methodik des erfolgten Experiments eingegangen. Danach werden in Kapitel acht die Ergebnisse präsentiert und in den letzten Kapiteln werden diese analysiert sowie unter Beachtung des aktuellen Forschungsstands interpretiert. Ebenfalls werden das Vorgehen, die Ergebnisse sowie die Arbeit selbst kritisch reflektiert.

2 Privatsphäre

In dieser Arbeit geht es darum, die Privatsphäre besser zu schützen. Doch wie ist die Privatsphäre definiert und gegen was schützt die Privatsphäre? In diesem Kapitel wird der Begriff Privatsphäre sowie dessen Risiken genauer angeschaut. Zudem wird in diesem Kapitel gezeigt, wie der Schutz der Privatsphäre in heutigen sozialen Netzwerken aussieht.

2.1 Überblick

Gemäss Altman (1981, S. 18) ist Privatsphäre «die selektive Kontrolle des Zugriffs auf sich selbst oder auf eine eigene Gruppe». Der Mensch sollte in der Lage sein, darüber zu entscheiden, welche Information von sich selbst oder einer Gruppe von Dritten eingesehen werden kann. In der Definition von Altman wird Privatsphäre als etwas beschrieben, das individuell ist und sich auch verändern kann. Ebenfalls schildert er, dass ein Mensch auch die Menge von Privatsphäre regulieren kann. Dabei ist allerdings zu beachten, dass wenn er zu wenig mitteilt, er sich allein fühlen kann. Im anderen Extrem kann er auch zu viel mitteilen, wodurch andere überrumpelt werden (Altman, 1981, S. 25).

Die Definition von Altman stammt aus dem Jahr 1975, in dem Computer und das Internet noch nicht für jeden zugänglich waren. Im Jahr 2021 haben schätzungsweise 65.6% der Weltbevölkerung Zugriff auf das Internet, von denen 53.6% aktive Nutzer und Nutzerinnen von sozialen Netzwerken bilden (We Are Social et al., 2021, S. 7). In der Schweiz sind es insgesamt 81.8% der Bevölkerung, die auf sozialen Netzwerken aktiv sind (We Are Social et al., 2021, S. 17). Durch die Nutzung des Internets und des Computers lassen sich Daten einfacher vervielfältigen und speichern als zu den Zeiten von Altmans Definition. Das ist darauf zurückzuführen, dass Informationen, die im Internet für andere sichtbar gemacht werden, einfach kopiert werden können von denen, mit denen sie geteilt wurden. Was Dritte mit dem so erlangten Wissen vornehmen, kann nicht überprüft werden. Diese Tatsache erlaubt es Internetnutzerinnen und -nutzern nicht, vollständig über den Personenkreis, mit dem Inhalte geteilt werden, sowie ihre Verwendung zu bestimmen. Ebenso kann auch nicht sichergestellt werden, dass alle Kopien des Inhaltes vollständig gelöscht wurden – zumindest kann sich der Nutzer oder die Nutzerin nicht vollständig versichern, dass keine digitalen Kopien mehr existieren (Rudin, 2003, S. 137–144). Es stellt sich die Frage, ob die Privatsphäre aufgrund der erzielten technologischen Fortschritte heute eine andere Bedeutung hat als vor 40 Jahren. Das verneinen Trepte und Dienlin (2015) in ihrer Arbeit: Es kam zwar nach ihnen zu wesentlichen Veränder-

ungen der Privatsphäre in der digitalen Welt, allerdings sind es keine neuen Vorgänge der Privatsphäre, die sich gewandelt haben, sondern bereits bekannte.

Es können nicht nur private Personen Daten missbrauchen, die auf ein soziales Netzwerk hochgeladen werden, sondern auch Firmen und Organisationen. So hat das Unternehmen Cambridge Analytica beispielsweise im Wahlkampf der Vereinigten Staaten anhand Facebook-Nutzer-/Nutzerinnendaten Wahlprofile erstellt – ohne die volle Kenntnis der User und Userinnen (Langer, 2018).

Die Privatsphäre kann in zwei Bereiche eingeteilt werden: den sozialen und den institutionellen. In letzterem geht es um den Schutz der eigenen Daten gegenüber einer Firma, die zum Beispiel einen Dienst zur Verfügung stellt. Hingegen handelt es sich bei der sozialen Privatsphäre um den Schutz gegenüber Personen, die bekannt oder auch unbekannt sind (Raynes-Goldie, 2010). In dieser Arbeit liegt der Fokus auf dem Schutz gegenüber Personen, d. h. auf der sozialen Privatsphäre und dem Missbrauch von persönlichen Daten, der in dieser entstehen kann.

2.2 Risiken beim Teilen von persönlichen Inhalten

In sozialen Netzwerken können sich Nutzerinnen und Nutzer mit anderen Personen auf der ganzen Welt vernetzen und frei austauschen. Dadurch wird es ihnen ermöglicht, sich selbst darzustellen. Diese Möglichkeit hat auch eine Schattenseite, denn durch die Veröffentlichung von persönlichen Informationen können verschiedene Risiken entstehen.

Ein Risiko bildet unter anderem das ‚Cyberstalking‘: Durch die Verfügbarkeit von Informationen im Internet erhalten Stalker/innen neue Möglichkeiten, ihren OpferInnen und Opfern nachzustellen. In einer Untersuchung von Dreßing, Bailer, Anders, Wagner und Gallas (2014, S. 62–65) wurde eine Online-Befragung zum Thema Cyberstalking durchgeführt. Von den 6379 konsultierten Personen gaben 43.3% an, dass sie schon einmal ungewollten Kontakt oder eine Belästigung online erlebt hatten. Bei 19.1% hielt dieser Zustand länger als zwei Wochen an und bei 8.4% bewirkte das Cyberstalking Angst. Die Täter/innen waren mit 69.9% meistens Bekannte. Die Folgen für die Opfer/-innen bildeten innere Unruhe, Misstrauen gegenüber anderen Personen, Schlafstörungen, ein Gefühl von Hilflosigkeit, Wut und Aggression. In der genannten Studie wird Cyberstalking als ein unter Berücksichtigung der Vielzahl der Internetnutzenden häufig auftretendes Vorkommen eingestuft.

Neben Cyberstalking ist auch sexuelle Belästigung eines der verbreiteten Risiken in sozialen Netzwerken. In einer Untersuchung von Golder, Jans, Venetz, Bohn und Herzog (2019) gaben 52% der befragten 16- bis 39-jährigen Frauen an, schon einmal uner-

wünschte sexuell eindeutige Nachrichten online erhalten zu haben. Bei den 40- bis 64-Jährigen waren es 26%, die mit einer solchen Nachricht konfrontiert worden waren. In einer regelmässig durchgeführten Online-Befragung bei Jugendlichen konnte herausgefunden werden, dass 44% der Jugendlichen schon einmal in sozialen Netzwerken von einer unbekannt Person mit sexuellen Absichten kontaktiert worden waren. Mädchen waren davon deutlich öfter betroffen als Jungen. Zudem steigt der Anteil von Betroffenen mit dem Alter, sprich ältere Jugendliche haben häufiger Erfahrungen mit sexueller Belästigung gemacht als jüngere Jugendliche. In der Studie konnte auch ein starker Anstieg des Anteiles an Jugendlichen erkannt werden, die mit sexueller Belästigung im Internet Erfahrung gemacht hatten. So lag ihr Anteil im Jahr 2010 noch bei 19%, heute beläuft er sich aber auf 44% (Bernath et al., 2020, S. 50–54). Es kann daraus abgeleitet werden, dass Jugendliche im Vergleich zu Älteren eher stärker betroffen sind von sexuellen Belästigungen im Internet, Tendenz steigend.

Besonders bei Jugendlichen stellt sich die Frage, ob sie die Risiken, die durch eine hohe Selbstoffenbarung entstehen, wahrnehmen können. Dies wurde bereits in zwei Studien beleuchtet, in denen das Bewusstsein Jugendlicher und junger Erwachsenen bezüglich möglicher Risiken der Veröffentlichung von Inhalten erhoben wurde. In beiden Studien wird bei Jugendlichen eine eher geringe Sorge um veröffentlichte Daten nachgewiesen (Niemann, Schenk, Teutsch, Wlach & Allgeier, 2012; Willemse, Waller, Süss, Genner & Huber, 2012). Zudem kann über die Jahre ein negativer Trend festgestellt werden. Beispielsweise sank der Anteil Jugendlicher, die sich Sorgen machen über ihre Sichtbarkeit, laut der JAMES-Studie im Zeitraum vom 2012 bis 2020 um 8% von 38% auf 30% (Bernath et al., 2020; Willemse et al., 2012). Dass der negative Trend des Risikobewusstseins von Jugendlichen mit der Zunahme an sexuellen Belästigungen von Jugendlichen im Internet zusammenhängt, kann weder bestätigt noch ausgeschlossen werden.

2.3 Einstellungen zum Schutz der Privatsphäre in sozialen Netzwerken

Auf jedem sozialen Netzwerk gelten andere Einstellungen bezüglich der Privatsphäre, die in diesem Unterkapitel erläutert werden sollen. Dabei werden vor allem die Einstellungsmöglichkeiten in Bezug auf die Inhalte sowie die Zielgruppe betrachtet. Die Untersuchung wird in der vorliegenden Arbeit auf die acht meistgenutzten sozialen Netzwerke beschränkt, in denen Inhalte öffentlich geteilt werden können. In der Schweiz sind dies YouTube (85.2%), Facebook (68.7%), Instagram (57.8%), LinkedIn (34.5%), Pinterest (32.6%), Twitter (27.3%), Snapchat (24.2%) und TikTok (19.7%) (We Are Social et al., 2021, S. 47). Bei Jugendlichen fällt diese Statistik ein wenig anders aus: Gemäss

JAMES-Studie der ZHAW (Zürcher Hochschule für Angewandte Wissenschaften) führen hier deutlich Instagram (93%) und Snapchat (91%) gefolgt von TikTok (74%), Pinterest (61%) und Facebook (50%) (Bernath et al., 2020, S. 35).

YouTube ist ein Online-Video-Portal, auf dem Videos geteilt und angesehen werden können (Taskin, 2015). Es gibt drei Arten von Videos, die eine Personen hochladen und teilen kann: Zum einen bestehen sogenannte öffentliche Videos, die von allen Personen auch ohne YouTube-Konto angesehen werden können. Zum anderen bestehen private Videos, die nur der Person, von der das Video hochgeladen wurde, und Menschen, die sie selbst ausgewählt hat, zugänglich sind. Die dritte Art bilden nicht gelistete Videos, auf die kann nur durch den direkten Link zugegriffen werden kann (Google LLC, o. D.).

Funktion	Privat	Nicht gelistet	Öffentlich
URL kann geteilt werden	Nein	Ja	Ja
Kann einem Kanalabschnitt hinzugefügt werden	Nein	Ja	Ja
Erscheint in den Suchergebnissen, in Listen mit ähnlichen Videos und in Empfehlungen	Nein	Nein	Ja
Wird auf deinem Kanal gepostet	Nein	Nein	Ja
Erscheint im Abofeed	Nein	Nein	Ja
Kann kommentiert werden	Nein	Ja	Ja

Abbildung 1: Übersicht der Privatsphäre-Einstellungen von YouTube. Quelle: Google LLC, o.D.

Facebook ist ein soziales Netzwerk, das zum Vernetzen und zum Chatten mit Freunden sowie Freundinnen aus der ganzen Welt genutzt wird (Wölwer, 2018). Nutzerinnen und Nutzern wird es ermöglicht, die Gruppe zu bestimmen, mit der ein Profil oder ein Inhalt (zum Beispiel ein Foto) geteilt werden soll. Facebook stellt seinen Nutzenden vier Optionen zur Auswahl: Sie können einen Inhalt mit jedem teilen. Bei dieser Möglichkeit ist kein Facebook-Account notwendig, um den Inhalt anzusehen, ein Internetanschluss genügt. Darauf folgt die Option «Freunde», über die ein Inhalt mit Freunden und Freundinnen geteilt wird. Wenn allerdings eine andere Person in diesem Beitrag markiert wird, können standardgemäss die Freunde der markierten Person diesen Beitrag auch sehen. Um dies zu verhindern, muss die Option «Freund von markierten Personen» in den benutzerdefinierten Einstellungen gezielt deaktiviert werden. Neben diesen Optionen kann der Inhalt auch nur mit sich selbst geteilt werden und es kann bei Facebook eine benutzerdefinierte Gruppe bestimmt werden, ihn einsehen kann. Dies gelingt über sogenannte Freundeslisten (Facebook Inc., o. D.-a).

Instagram wird zum Teilen von Fotos und Videos genutzt und existiert seit 2010. Sie wurde 2012 vom Facebook-Konzern gekauft und gehört somit seither zu diesem (Aschermann, 2019). Auf Instagram existieren nicht die gleichen Optionen für die Einstellung der Privatsphäre wie bei Facebook. Einzig die Möglichkeit, das Konto und somit alle Beiträge auf «privat» zu setzen, liegt vor. Nach diesem Schritt können nur bestätigte Abonnentinnen und Abonnenten Beiträge sehen. Eine Einstellung auf Ebene eines Beitrages fehlt bei Instagram (Facebook Inc., o. D.-b). Seit dem 30. November 2018 kann für die Story-Funktion eine Gruppe aus engen Freunden erstellt werden, um einzuschränken, wer eine Story sehen kann. Andere Nutzende können die Liste nicht betrachten und somit dieser auch nicht selbstständig beitreten (Facebook Inc., 2018).

LinkedIn ist eines der grössten Berufsnetzwerke, auf dem Personen Kontakte und Beziehungen für ihre Karriere pflegen (Schneider, 2019). Es bietet die Möglichkeit, Privatsphäre-Einstellungen für Angaben im Profil, Kontakte, Profilbild, Nachname, Geburtsdatum und Beiträge, die der/die Nutzer/in selbst im Netzwerk teilt, vorzunehmen (LinkedIn Corporation, o. D.-b). Bei den Beiträgen gilt es, zwischen fünf Optionen zu wählen. So können Inhalte mit jedem ohne LinkedIn-Account geteilt werden. Zudem können sie auch nur Kontakten (direkten Kontakten), Gruppenmitgliedern oder Veranstaltungsteilnehmenden bereitgestellt werden (LinkedIn Corporation, o. D.-a). Neben den Beiträgen kann auch im Profil genau bestimmt werden, wer was sehen darf. Je nach Art der Information stehen unterschiedliche Einstellungen zur Auswahl (LinkedIn Corporation, o. D.-b).

Auf Twitter können kurze Nachrichten namens Tweets mit maximal 140 Zeichen mit Freundinnen und Freunden oder der Community geteilt werden (Bekker, 2016). Hier besteht die Möglichkeit, Personen anhand ihrer E-Mail-Adresse oder ihrer Telefonnummern zu finden. Diese Option lässt sich in den Einstellungen deaktivieren. Die E-Mail-Adresse und die Telefonnummer sind auf Twitter allerdings nicht öffentlich einsehbar (Twitter Inc., o. D.-a). Das Profil und die Tweets können entweder «öffentlich» oder «geschützt» sein. Wenn sie auf «öffentlich» eingestellt sind, kann jede/r die Tweets und das Profil sehen. Wenn in den Einstellungen «geschützt» gewählt wird, können nur Follower Inhalte und das Profil finden. Nur wenn ein Link erstellt wird, der für den konkreten «Tweet» gilt, können auch in diesem Fall alle (die im Besitz dieses Links sind) auf ihn zugreifen. Zudem muss jede/r neue Follower bestätigt werden. Es ist ihnen auch nicht möglich, «Tweets» zu teilen. Ferner lassen sie sich nicht über Google oder andere Suchmaschinen finden (Twitter Inc., o. D.-b).

Bei Snapchat ist standardmässig eingestellt, dass nur Freunde, die ein/e Nutzer/in selbst hinzugefügt hat, Stories ansehen und Kontakt mit der sie erstellenden Person aufnehmen

können. Wenn die Einstellungen geändert werden sollen, kann selektiert werden, wer Kontakt aufnehmen, Benachrichtigungen senden, die Story ansehen, den Standort erkennen, ein sogenanntes «Cameos-Selfie» verwenden und das Profil als Vorschlag angezeigt bekommen soll. Selektiert werden kann jeweils «Freunde» oder «jeder» (Snap Inc., o. D.).

Pinterest ist eine Sammlung aus Online-Pinnwänden, die mit verschiedenen Interessen gefüllt sowie mit Freundinnen und Freunden geteilt werden können (Predan-Hallabrin, 2019). Nutzer/innen können ihr Konto hier nicht vollständig auf privat stellen, die Pinnwände können aber geheim gehalten werden, damit diese niemand sehen kann. Auch kann das Profil vor Suchmaschinen verborgen werden. Pinterest empfiehlt Personen, die mehr Privatsphäre haben möchten, ihren Namen zu ändern oder geheime Pinnwände zu verwenden (Pinterest Inc., o. D.).

In der TikTok-App lassen sich die Privatsphäre-Einstellungen bezüglich der Kommentare und den Funktionen Duett, Reagieren, Stitch, Direktnachrichten und Anzeigen des Kontos sowie einzelne Inhalte definieren. Somit kann der Nutzende einstellen, ob Inhalte jeweils nur für sich selbst, «privat», mit der Option «Freunde» für seine Freundinnen und Freunde oder für alle «öffentlich», sprich für alle Personen mit einem Internetanschluss, einsehbar sein sollen. Wenn das Profil privat ist, steht letztere Option nicht zur Auswahl, sondern es kann die Möglichkeit «Follower» selektiert werden, womit der Zugriff auf diejenigen Personen beschränkt wird, die dem Profil folgen (ByteDance Ltd., o. D.-b). Seit dem Januar 2021 hat ByteDance Ltd. zusätzliche Schutzfunktionen für Minderjährige hinzugefügt, um ihnen eine altersangemessene Erfahrung zu bieten. Diese Schutzfunktion besteht aus einigen Einstellungen, die standardmässig restriktiv gesetzt oder deaktiviert werden (ByteDance Ltd., o. D.-a).

Datenschutzeinstellung	Nutzer*innen unter 16 Jahren	Nutzer*innen im Alter von 16 und 17 Jahren
Privates Konto	Dein Konto wird privat gemacht. Das bedeutet, dass nur von dir genehmigte Nutzer*innen dir folgen und deine Videos anschauen können. Du kannst dein Konto öffentlich machen.	Dein Konto wird standardmäßig öffentlich gemacht. Du kannst dein Konto privat machen, wenn du möchtest.
Schlage anderen dein Konto vor	Diese Einstellung wird deaktiviert . Das bedeutet, dass dein Konto anderen Nutzer*innen nicht vorgeschlagen wird. Du kannst die Einstellung aktivieren .	Diese Einstellung wird aktiviert . Du kannst die Einstellung deaktivieren , damit dein Konto anderen Nutzer*innen nicht mehr vorgeschlagen wird.
Erlaube das Herunterladen deiner Videos	Diese Einstellung wird deaktiviert und es ist keine Änderung möglich.	Diese Einstellung wird deaktiviert . Du kannst die Einstellung aktivieren , wenn du anderen Nutzer*innen erlauben möchtest, deine Videos herunterzuladen.
Wer mit deinen Videos ein Duett aufführen kann	Diese Einstellung wird auf „ Nur ich “ gesetzt. Nur du kannst ein Duett mit deinen Videos aufführen. Die Einstellung kann nicht geändert werden.	Diese Einstellung wird auf „ Freunde “ gesetzt. Du kannst die Einstellung auf „ Nur ich “ oder „ Alle “ setzen, wenn du möchtest.
Wer mit deinen Videos ein Stitch aufführen kann	Diese Einstellung wird auf „ Nur ich “ gesetzt. Nur du kannst ein Stitch mit deinen Videos aufführen. Die Einstellung kann nicht geändert werden.	Diese Einstellung wird auf „ Freunde “ gesetzt. Du kannst die Einstellung auf „ Nur ich “ oder „ Alle “ setzen, wenn du möchtest.
Wer deine Videos kommentieren kann	Diese Einstellung wird auf „ Freunde “ gesetzt. Das bedeutet, dass nur Nutzer*innen, die dir folgen und denen du auch folgst, deine Videos kommentieren können. Du kannst die Einstellung auf „ Niemand “ setzen, damit andere Nutzer*innen deine Videos nicht mehr kommentieren können.	Diese Einstellung wird auf „ Alle “ gesetzt. Du kannst dies jederzeit ändern, wenn du einschränken möchtest, wer deine Videos kommentieren kann.

Abbildung 2: Datenschutzeinstellungen für Minderjährige auf TikTok. Quelle: ByteDance Ltd., o.D.-a

Auf sozialen Netzwerken bestehen verschiedene Möglichkeiten, die Privatsphäre der Nutzenden zu schützen, wie zuvor erläutert wurde. Unklar ist es, ob die Nutzenden diese Optionen kennen und ihre jeweiligen Risiken ausreichend abschätzen können. In einer Studie mit 200 Personen, die Facebook nutzen, konnte beispielsweise festgestellt werden, dass nur 37% der Inhalte so eingestellt wurden, wie es von der der die Einstellung vornehmenden Person intendiert wurde. Meistens wurden die Inhalte, die falsch eingestellt waren, mit mehr Personen als gedacht geteilt (Liu, Gummadi, Krishnamurthy & Mislove, 2011, S. 1).

3 Selbstoffenbarung

Die Selbstoffenbarung ist ein Bestandteil der Untersuchung dieser Bachelorarbeit, darum wird die Selbstoffenbarung in diesem Kapitel genauer untersucht. Dabei wird zuerst der Begriff genauer erläutert. Folglich wird verglichen, ob und wie sich die Online- und Offline-Selbstoffenbarung unterscheidet. Zu guter Letzt werden in diesem Kapitel die Einflüsse auf die Selbstoffenbarung angeschaut.

3.1 Begriffsbestimmung

«Selbstoffenbarung kann definiert werden als jede Information über sich selbst, die Person A verbal an eine Person B weitergibt.» (Cozby, 1973, S. 73) Die Selbstoffenbarung ist für einen Menschen bedeutend in Beziehungen mit anderen. Wenn jemand zu wenig von sich preisgibt, kann dies einer Beziehung schaden, da es von vielen Personen als unangemessen angesehen wird. Aber auch eine zu hohe Selbstoffenbarung kann schädlich sein für Beziehungen, da sich die andere Person durch diese bedroht fühlen könnte in ihrer Privatsphäre (Cozby, 1972, S. 157–159).

Neben Vorteilen für menschliche Beziehungen löst die Selbstoffenbarung auch Vorteile für gewisse Hirnregionen aus. Wenn Menschen Informationen über sich selbst preisgeben, reagiert das mesolimbische Belohnungssystem (Tamir & Mitchell, 2012, S. 8038), das für die Erzeugung von Belohnungsstoffen beziehungsweise lusterzeugenden Stoffen zuständig ist. Ein bekanntes Beispiel entsprechender Stoffe bildet Dopamin, das dafür sorgt, dass der Mensch Motivation und Lust empfindet (Biesinger, 2018, S. 63). Das bei der Selbstoffenbarung ausgeschüttete Dopamin ist etwa gleich hoch, wie wenn ein Mensch Essen zu sich nimmt oder Geschlechtsverkehr mit einer anderen Person hat. Dadurch entsteht eine hohe intrinsische Motivation zur Selbstoffenbarung (Tamir & Mitchell, 2012, S. 8041).

Sowohl von Beziehungen als auch von der eigenen Motivation ist die Selbstoffenbarung ein zentraler Bestandteil, allerdings kann sie sich von Person zu Person unterscheiden (Cozby, 1973, S. 75). In der Arbeit von Cozby (1973, S. 75) werden die Basisparameter der Selbstoffenbarung definiert. Unter diese fallen Umfang oder Menge und Tiefe beziehungsweise Intimität der mitgeteilten Information und die Dauer ihrer Beschreibung.

3.2 Online- versus Offline-Selbstoffenbarung

Es ergibt sich die Frage, ob die geschilderten Erkenntnisse über die Belohnung der Selbstoffenbarung auch Gültigkeit haben, wenn Informationen online geteilt werden. Ein

Unterschied besteht hier im Zeitfaktor, da verstärkt geplant beziehungsweise abgewogen wird, welche Information wie preisgegeben werden sollen. In sozialen Netzwerken kann viel Zeit damit verbracht werden, Inhalte zu optimieren und sich zu überlegen, wer diese sehen darf. Bei einem physischen Gespräch sind entsprechende Gedanken nicht möglich (Krämer & Haferkamp, 2011, S. 129). Von dieser Tatsache abgesehen sind die Bekanntheit und der Erfolg von sozialen Netzwerken, von denen die Selbstoffenbarung persönlicher Informationen ein elementarer Bestandteil ist, ein Indikator dafür, dass das bekannte Selbstoffenbarungsverhalten und seine Vorteile auch in sozialen Netzwerken Gültigkeit haben (Krämer & Schäwel, 2020, S. 68).

Heute ermöglichen soziale Netzwerke das Teilen von persönlichen Informationen in grossem Umfang. Die Effekte der Selbstoffenbarung werden von entsprechenden Plattformen sogar bewusst genutzt: Soziale Netzwerke erstellen selbst keine Inhalte, sondern sind abhängig von den Inhalten, die ihre Nutzerinnen und Nutzer tagtäglich auf ihnen veröffentlichen. Ihr Geschäftsmodell basiert darauf, möglichst viele Nutzende möglichst lange zu behalten. Jedes soziale Netzwerk baut somit zu einem Teil auf der Selbstoffenbarung einzelner Personen auf. Durch diese entsteht der Inhalt, der die Nutzenden motiviert, auf dem entsprechenden sozialen Netzwerk Zeit zu verbringen (Abramova et al., 2017, S. 1).

3.3 Umfang der Selbstoffenbarung in sozialen Netzwerken

In der Studie von Taddicken (2011, S. 296–298) wurden deutsche Internetnutzende zum Selbstoffenbarungsverhalten befragt. Informationen wie Vornamen, E-Mail-Adresse, Geburtstag und Beruf werden nach ihren Erkenntnissen von Nutzerinnen und Nutzer in sozialen Netzwerken mehrheitlich geteilt. Aber auch Wissen, das als intim gilt – beispielsweise die eigene Gefühlslage – wurde von 23.4% schon häufig veröffentlicht. Die Nutzungshäufigkeit, die Bindung zu sozialen Netzwerken und das Bildungsniveau haben einen Einfluss auf die Menge des Geteilten: Durch eine häufige Nutzung von sozialen Netzwerken sind Personen verstärkt dazu geneigt, Inhalte preiszugeben. Allerdings je mehr verschiedene Netzwerke eine Person nutzt, desto weniger persönliche Informationen gibt diese preis. Allerdings konnte nicht ausgeschlossen werden, dass die Anzahl an Freundinnen und Freunden die Selbstoffenbarung beeinflusst, denn es könnte vorkommen, dass Personen aufgrund des Personenkreises, in dem sie Inhalte teilen, viel posten. Neue soziale Netzwerke haben eine moderne Konstruktionsweise: Bei sozialen Netzwerken wie Instagram oder Snapchat ist es eher kontraproduktiv für die Popularität, wenn sich eine Person stark schützt. Je mehr Informationen geteilt werden, desto attraktiver

wird das Profil auf dem Netzwerk. Diese Attraktivität zeigt sich in sogenannten «Likes». Vor allem in neuen sozialen Netzwerken ist die Anzahl der Likes bedeutend für die Popularität. Daher sinkt vermutlich auch der Anteil der Jugendlichen, die Einstellungen zum Schützen der Privatsphäre aktivieren: Im Jahr 2014 waren es noch 81%, im Jahr 2020 jedoch nur noch ca. 66%. Das bedeutet eine Verringerung um 18.5% (Bernath et al., 2020, S. 50–51).

3.4 Bedürfnis nach Popularität

Popularität wird in dieser Arbeit gemäss folgender Definition ausgelegt: «der Fakt, dass jemand oder etwas gemocht, geschätzt oder unterstützt wird von vielen Personen» (Cambridge University, o. D.). Das heisst, eine Person gilt als populär, wenn sie von einer Gruppe von Menschen gemocht wird und in dieser bekannt ist. Unter dem Bedürfnis nach Popularität wird in dieser Arbeit das Streben nach dem soeben definierten Status verstanden.

Dass Popularität Einfluss auf das Verhalten in sozialen Netzwerken nimmt, zeigen zahlreiche Untersuchungen (Utz, Tanis & Vermeulen, 2012; Christofides, Muise & Desmarais, 2009; Chen, Widjaja & Yen, 2015). Zusätzlich konnte ein positiver Zusammenhang zwischen der Selbstoffenbarung und dem Bedürfnis nach Popularität nachgewiesen werden (Cheung et al., 2015; Christofides et al., 2009; Hallam & Zanella, 2017; Hollenbaugh & Ferris, 2014; Ng, 2014; Utz et al., 2012). Diese Verbindung lässt sich möglicherweise damit erklären, dass Personen, die ein hohes Bedürfnis an Popularität aufweisen, eine gewisse Reichweite und Aufmerksamkeit benötigen. Aufgrund der im letzten Unterkapitel erwähnte Konstruktionsweise der Plattformen lassen sich diese nur durch eine starke Selbstoffenbarung erreichen (Bernath et al., 2020, S. 50–51). Das bedeutet, dass viele Inhalte wie Bilder und Interessen aus dem privaten Leben geteilt werden müssen (Christofides, Muise & Desmarais, 2009, S. 343). Diese Vermutung wird dadurch bestärkt, dass bei Personen mit einem hohen Bedürfnis nach Popularität eine durchaus hohe Bewusstheit über die Privatsphäre und die Risiken für diese bestehen kann. Allerdings möchten entsprechende Personen ihre Reichweite nicht künstlich verschlechtern, so verzichten sie auf Einstellungen, die ihrem Schutz dienen (Christofides, Muise & Desmarais, 2009, S. 343–344).

3.5 Soziales Umfeld

Der Einfluss des sozialen Umfelds auf das Selbstoffenbarungsverhalten wurde in mehreren Studien nachgewiesen (Acquisti, John & Loewenstein, 2012; Barak & Gluck-Ofri,

2007; Lee, Hsiao, Weng & Chen, 2020; Taddicken, 2014). Taddicken (2014) konnte den Trend feststellen, dass wenn Freundinnen und Freunde oder Bekannte einer Person auf einem sozialen Netzwerk aktiv sind, diese hier mehr persönliche Informationen teilt. Allerdings ist es unklar, ob die Selbstoffenbarung der Freundinnen und der Freunde/der Bekannten Einfluss darauf nimmt, den aus der Studie von Barak und Gluck-Ofri (2007) geht hervor, dass ein solcher Effekt bei unbekanntem Personen existiert. In ihr wurde in Foren untersucht, wie Personen auf Einträge antworten. Hat ein/e User/in persönliche Informationen in einem Post preisgegeben, enthielten auch die Antworten mehr dieser. Daher kann nicht ausgeschlossen werden, dass das Selbstoffenbarungsverhalten auch durch Personen einer unbekanntem Gruppe beeinflusst werden kann. In der Studie von Lee et al. (2020) wurde der Zusammenhang zwischen dem Beziehungskapital und der Selbstoffenbarung untersucht, es konnte eine positive Verbindung bestätigt werden.

3.6 Privacy Paradox

Viele Personen geben an, besorgt um den Schutz ihrer persönlichen Daten zu sein. Das zeigt beispielsweise eine Umfrage in Deutschland, in deren Rahmen nur drei Prozent der Befragten meinten, dass es ihnen egal sei, was mit ihren Daten passiert. Das bildet grundsätzlich eine gute Voraussetzung für einen soliden Datenschutz, doch geben viele Personen wesentlich mehr persönliche Daten preis, als sie in der Befragung schilderten (Gerber, Volkamer & Gerber, 2017, S. 142). Das widersprüchliche Verhalten, das Personen offenbaren, die meinen, sich um ihre Daten Sorgen zu machen, aber diese trotzdem teilen, wird unter dem Begriff «Privacy Paradox» erfasst (Young & Quan-Haase, 2013, S. 479).

Das Privacy Paradox wurde bereits in mehreren Studien untersucht. In einigen konnte ein fehlender Zusammenhang zwischen den Sorgen um die Privatsphäre und der Menge an geteilten Informationen festgestellt werden (Hughes-Roberts, 2013; Reynolds, Venkatanathan, Gonçalves & Kostakos, 2011; Taddicken, 2014; Tufekci, 2007). Auch geht es aus der Forschung hervor, dass ein entsprechender Zusammenhang beziehungsweise ein solches Paradox gar nicht existiert (Blank, Bolsover & Dubois, 2014; Boyd & Hargittai, 2010; Christofides et al., 2009; Lutz & Strathoff, 2014; Young & Quan-Haase, 2013). Somit scheint in diesem Punkt keine Einigkeit zu bestehen. Abgeschlossen ist die Erforschung des Privacy Paradox allerdings noch nicht, so werden laufend neue Aspekte geprüft (Kokolakis, 2017, S. 130).

Eine mögliche Erklärung für diese verschiedenen Resultate könnte darin liegen, dass die Privatsphäre stark kontextabhängig ist (Morando, Iemma & Raiteri, 2014, S. 7–8). Das

zeigt auch das Experiment von Norberg, Horne und Horne (2007, zitiert nach Kokolakis, 2017, S. 127), in dessen Rahmen Forschende Studierende dazu befragten, welche Informationen sie teilen würden. Zu einem späteren Zeitpunkt wurden letztere im Rahmen einer angeblichen anderen Studie einer Bank kontaktiert. Sie mussten erneut Angaben über sich treffen. Dabei stellte sich heraus, dass sie deutlich mehr preisgaben als bei der ursprünglichen Befragung. Dieses Experiment zeigt einen möglichen Zusammenhang zwischen dem Kontext und der Einstellung zur Privatsphäre.

Neben den Kontext könnte auch das Zielpublikum entscheidend sein. In einer anderen Untersuchung konnte beispielsweise festgestellt werden, dass Personen ihre Daten mehr gegen Personen als gegen Unternehmen schützen (Young & Quan-Haase, 2013, S. 492). Verstärkt wird diese Vermutung durch die steigenden Nutzerzahlen von Facebook trotz negativer Schlagzeilen zum Datenschutz. Einen bekannten Fall dieser bildet die Cambridge-Analytica-Affäre, in deren Rahmen die Firma anhand illegal beschaffter Daten auf Facebook Wählerprofile erstellte. Dieser Fall sorgte für negative Schlagzeilen über das soziale Netzwerk (Betschon, 2018). Nichtsdestotrotz konnte Facebook seine Nutzerzahlen laufend steigern (Facebook Inc., 2021). Es wäre zu erwarten gewesen, wenn nach diesen Schlagzeilen die Nutzerzahlen eingebrochen wären. Dass es nicht dazu kam, könnte daran liegen, dass die Auswirkung eines Datenschutzeskandals wie Cambridge Analytica Personen nicht so stark bemerken, wie wenn jemand ihre persönlichen Informationen aktiv missbraucht.

Zur Erklärung des Paradoxons liegen unterschiedliche Versuche vor. Eine dieser Erklärungen basiert auf der falschen Risikoeinschätzung. Es ist schwer, sich ein Risiko und dessen Folgen vorzustellen, wenn diese die betrachtende Person selbst noch nicht erlebt hat – auch wenn sie ihr grundsätzlich bekannt sind. So kann die Gefahr der Preisgabe von sensiblen Daten schwer eingesehen werden. Hingegen lassen sich die Vorteile gut vorstellen, da diese bereits erlebt wurden (Gerber et al., 2017, S. 155–156).

Ein weiterer Ansatz besteht im Unwissen über die Einstellungsmöglichkeiten zum Privatsphärenschutz. Zwar gaben bei einer Befragung 91% der Interviewten an, sich mit den Einstellungen auszukennen (Debatin, Lovejoy, Horn, & Hughes, 2009, S. 93), allerdings konnte nicht erkannt werden, ob die Befragten hier sich selbst nicht besser einschätzten, als sie es eigentlich waren. Das ist möglich, denn in diesem Bereich scheinen sich Nutzer/innen gerne zu überschätzen (Kokolakis, 2017, S. 129). Das zeigt auch ein Experiment, in dem analysiert wurde, wie Sicherheitseinstellungen gewünscht und tatsächlich getroffen werden. Es konnte festgestellt werden, dass sie User/innen in weniger als 40% der Fälle korrekt eingestellt hatten (Liu et al., 2011, S. 65).

Es gibt wie erwähnt unterschiedliche Resultate zum Privacy Paradox. Die Gründe für entsprechende Differenzen liegen im Kontext, aber auch in den verschiedenen Methoden und Setups, die im Rahmen seiner Untersuchung genutzt wurden (Kokolakis, 2017, S. 127). Es erfolgten stark unterschiedliche Untersuchungen zu diesem Thema, deren Thesen sich teilweise sogar widersprechen. Eindeutig ist es, dass die Forschung zum komplexen Thema Privacy Paradox noch nicht abgeschlossen ist.

4 Nudging

Mit Nudging beziehungsweise Digital Nudging soll in dieser Arbeit untersucht werden, ob dadurch Personen verleitet werden können, weniger Daten zu offenbaren. Daher gehört Nudging beziehungsweise der Nudge zu einem wichtigen Bestandteil dieser Arbeit. In dem folgenden Kapitel wird der Begriff Nudging definiert, sowie die Nudging Theorie genauer betrachtet. Folglich wird auch der Kritik an Nudging angeschaut und am Schluss wird das Digital Nudging erläutert.

4.1 Eingrenzung

Eine kleine Fliege auf einem Urinal bringt Männer dazu, beim Urinieren besser zu zielen. Das konnte zum ersten Mal am Flughafen in Amsterdam festgestellt werden. Was als ein scheinbar unwesentliches Detail wirkt, erbringt einen starken Nutzen. Dieses Beispiel zeigt, dass alles einen Einfluss auf die Entscheidung eines/einer Einzelnen haben kann. Auf dieser Erkenntnis basiert die Theorie des Nudgings (Thaler & Sunstein, 2009).

Unter dem Begriff des Nudgings wird das Erteilen eines leichten Anstosses zu einer Entscheidung verstanden – in die Richtung, die für den/die Entscheidende/n am besten ist. Durch einen Nudge können private Unternehmen, aber auch der Staat Personen mit einer leichten Veränderung der Auswahl einfach beeinflussen. Das Ziel sollte es dabei bilden, den Menschen zu erinnern, zu warnen oder aufmerksam zu machen, eine für sich bessere beziehungsweise rationalere Entscheidung zu treffen. Die Methode soll hingegen nicht primär den eigenen Interessen eines Unternehmens oder Staates dienen. So sollte der sogenannte libertäre Paternalismus Anwendung finden (Thaler & Sunstein, 2009).

4.2 Libertärer Paternalismus

Der Begriff «libertärer Paternalismus» ist aus den Komponenten «Libertarismus» und «Paternalismus» zusammengesetzt. Der Libertarismus wird als die Möglichkeit des Menschen eingegrenzt, über seine Entscheidungen und Handlungen selbst zu bestimmen, die niemand – so zum Beispiel auch nicht der Staat – übernehmen soll (Boaz, 2021). Hingegen wird er Paternalismus als «der Eingriff in die Handlungsfreiheit einer Person [definiert], der durch Gründe gerechtfertigt ist, die sich ausschliesslich auf das Wohlergehen, das Wohl, das Glück, die Bedürfnisse, die Interessen oder die Werte der Person beziehen, die genötigt wird» (Dworkin, 1972, S. 65).

Die beiden Begriffe widersprechen sich in ihrer Auslegung, da im Libertarismus eine Unterbindung der Handlungsfreiheit einer Person, wie sie im Paternalismus vorgesehen ist, nicht toleriert wird. Doch unabhängig von der genauen Definition der beiden Wörter stellt der libertäre Paternalismus keine Art von Paternalismus in der Definition dar, denn bei diesem werden keine Handlungsoption verboten oder verschlechtert (Sunstein & Thaler, 2003, S. 1162). Das Ziel des libertären Paternalismus bildet es, den Menschen zwar frei entscheiden zu lassen, aber diese Entscheidung leicht in eine für die Person bessere Richtung zu leiten. Ein Beispiel dieses Vorgangs bildet die Essensanordnung in einer Schulkantine: Hier könnte durch bewusste Entscheidungen dafür gesorgt werden, dass sich die Kinder gesünder ernähren. Wenn ein Kind trotzdem etwas Ungesundes essen möchte, sollte es aber die Möglichkeit haben, dies ohne erhöhten Aufwand zu tun (Thaler & Sunstein, 2009).

Personen, die den libertären Gedanken verfolgen, nehmen häufig an, dass Menschen immer rational handeln; sie glauben an einen Homo oeconomicus. Dieser verhält sich immer rational und entscheidet entsprechend ohne andere Einflüsse. In der Praxis handelt der Mensch oft nicht wie ein Homo oeconomicus, wie es sich beispielsweise in der Ernährung zeigt (Thaler & Sunstein, 2009): Viele scheinen sich hauptsächlich ungesund zu ernähren, denn 42% der Schweizer Bevölkerung waren im Jahr 2017 übergewichtig oder adipös (Bundesamt für Statistik, 2018). Verursachen können Übergewichtigkeit und Adipositas vor allem Diabetes, Herz-Kreislauf-Erkrankungen oder sogar einige Krebsarten. Nichtsdestotrotz entscheiden sich Personen gegen eine ausgewogene Ernährung. Es ist anzumerken, dass sich nicht alle übergewichtigen und adipösen Personen aufgrund ihrer Ernährung oder aus fehlender Aktivität heraus in diesem Zustand befinden (Bundesamt für Gesundheit, o. D.-a).

Auch beim Konsum von Tabak zeigt sich ein ähnliches Bild: Obwohl dieser bekannterweise als eine Ursache verschiedener Krebsarten sowie Herz-Kreislauf-Krankheiten gilt sowie für die Verringerung der Lebenserwartung verantwortlich ist, konsumierten im Jahr 2017 27.1% der Schweizer Bevölkerung regelmässig Tabak. Die Folgen sind rund 9500 Todesfälle pro Jahr. Im Vergleich starben 2012 insgesamt 301 Personen aufgrund eines Verkehrsumfalles (Bundesamt für Gesundheit, o. D.-b). Ungefähr jede/r vierte/r Schweizer/in entscheidet sich bezüglich des Konsums von Tabak folglich nicht so, wie es im Konzept des Homo oeconomicus vorgesehen ist.

Wie es anhand der Beispiele des Tabakkonsums und der Übergewichtigkeit in der Schweiz zu erkennen ist, entscheiden Menschen nicht immer so, wie es für sie und in diesem Beispiel ihre Gesundheit am besten wäre (Thaler & Sunstein, 2009). Entsprech-

ende Fehlentscheidungen kommen nicht zufällig zustande, sondern sind Bestandteile ihres Wesens. Ein Grund dieser menschlichen Fehlbarkeit liegt an der Denkweise: Der Mensch denkt mit zwei Systemen, dem automatischen und dem reflektierenden System, auch System 1 und System 2 genannt (Kahneman & Schmidt, 2016; Thaler & Sunstein, 2009). System 1 bzw. das automatische System arbeitet, wie es sein Name vermuten lässt, vollkommen autonom. Hingegen benötigt System 2 die volle Aufmerksamkeit der Person. Es ist folglich beispielsweise schwer möglich, eine komplexe Mathematikaufgabe zu lösen und sich gleichzeitig auf den Verkehr einer stark befahrenen Strasse zu konzentrieren (Kahneman & Schmidt, 2016).

In vielen ökonomischen Modellen wird davon ausgegangen, dass der Mensch immer mit dem System 2 denkt, d. h. sich bei einer Entscheidung bewusst Gedanken macht und nicht sein «Bauchgefühl» verwendet oder sogar Annahmen trifft, ohne sie belegende Statistiken oder Untersuchungen zu kennen. Dies entspricht in vielen Fällen nicht der Realität (Thaler & Sunstein, 2009). Doch Thaler und Sunstein (2009) verurteilen mit dem libertären Paternalismus nicht jeden Konsum von Ungesundem oder jedes irrationale Verhalten. Es geht vielmehr darum, die Entscheidungen von Menschen mithilfe von Nudges teilweise zu verbessern, indem ihnen ein Anstoß in die richtige Richtung geboten wird.

4.3 Kritik

Neben Befürworterinnen und Befürwortern der Theorie des libertären Paternalismus von Sunstein und Thaler gibt es auch Kritiker/innen dieser. In diesem Unterkapitel werden als Beispiele zwei Kritikpunkte erwähnt und nachfolgend mit der Theorie des Nudgings verglichen.

Es wird beispielsweise kritisiert, dass die Personen, die Nudges erschaffen, d. h. als Entscheidungsarchitekten und -architektinnen agieren, nicht in der Lage seien, vollkommen zu wissen, welche Option diejenige ist, die im besten Interesse des betroffenen Menschen steht. Das könnte von aussen auch nicht festgestellt werden (White, 2013, S. 64). Ein anderes Argument gegen den libertären Paternalismus beschreiben Drerup und Voloj Dessauer (2016) in ihrem Artikel: Sie vermuten aufgrund der Anzahl an verschiedenen Personen, dass es unmöglich sei, zu wissen, ob ein Nudge immer eine Entlastung darstellt: Für manche Personen könnte er auch eine Einschränkung bedeuten.

Argumente, wonach nicht alle Vorlieben erkannt oder nicht alle Transaktionskosten gekannt werden können, haben ihre Berechtigung. Doch Thaler und Sunstein (2009) erwähnen, dass auch unbewusst viele Nudges entstehen können. Ein Beispiel dessen bil-

det der Fall, dass ein/e Arbeitgebende/r das Gehalt zum Beispiel alle zwei Wochen auszahlt und damit die Angestellten unbewusst dazu bringt, mehr zu sparen (Thaler & Sunstein, 2009). Zudem sei es nachweisbar, dass viele Menschen auch ohne Nudges teilweise nicht die Optionen wählen, die sie eigentlich wollen. Das zeigt auch das Experiment von Liu et al. (2011, S. 65), in dem weniger als 40% der Probanden und der Probandinnen die gewünschten Sicherheitseinstellungen korrekt umsetzten.

Daher können Nudges durchaus hilfreiche, sinnvolle Anstöße bilden, die dabei helfen, Entscheidungen besser zu treffen oder sich eher für die gewollte Option zu entscheiden. Dennoch werden, wie es der Begriff auch vermuten lässt, Ansätze des Paternalismus im Konzept übernommen, da Menschen verleitet werden, die Option zu wählen, die nach dem Nudge zu favorisieren ist. Zu betonen ist, dass im libertären Paternalismus keine Optionen verschlechtert oder sogar verboten werden. Die Person kann somit stets vom Nudge abweichend entscheiden, sofern sie das möchte, wodurch ihre Entscheidungsfreiheit gewährleistet bleibt (Sunstein & Thaler, 2003, S. 1162–1163).

4.4 Digital Nudging

Immer mehr alltägliche Aufgaben können mithilfe eines Computers oder eines Smartphones online erledigt werden – beispielsweise Bankgeschäfte, die Essensbestellung oder der wöchentliche Einkauf. Dadurch entstehen laufend neue Interaktionsmöglichkeiten mit Personen. Über Webseiten oder mobile Applikationen werden neue Wege geschaffen, Entscheidungen zu treffen, aber es gibt auch neue Möglichkeiten für Entscheidungsarchitekten und -architektinnen, Nudges zu kreieren. In der Online-Umgebung ist jede Entscheidung bewusst oder unbewusst mit Nudges verknüpft (Weinmann et al., 2016, S. 433–434).

Weinmann et al. (2016, S. 433) definieren den Gebrauch von entscheidungsbeeinflussenden Elementen in der Gestaltung von Benutzeroberflächen als Digital Nudging. Nach Schär und Stanoevska-Slabeva (2019, S. 2–3) ist diese Auslegung zu stark eingeschränkt. Interaktionsmöglichkeiten in der digitalen Welt bestehen laut ihnen heute nicht nur über einen Bildschirm, denn es ist beispielsweise möglich, mit einem Sprachassistenten (wie Siri, Alexa oder Google) oder mit einem Roboter zu interagieren, ohne eine grafische Oberfläche zu bedienen. Daher definieren sie Digital Nudging in Anlehnung an Gregor und Lee-Archer (2016) sowie Mirsch, Lehrer und Jung (2018) als «durch Informations- und Kommunikationstechnologie unterstütztes Nudging, das versucht, Entscheidungen, Urteile und Verhalten in einer vorhersehbaren Weise zu beeinflussen, indem [die] [...] kognitiven Grenzen, Vorurteile, Routinen und Gewohnheiten die Individuen da-

ran hindern, in der digitalen Sphäre zu ihrem eigenen Vorteil zu handeln. Dabei werden keine Optionen verboten oder hinzugefügt, Anreize nicht wesentlich verändert [und es werden] keine rationalen Argumentationen vor[gegeben].» (Schär & Stanoevska-Slabeva, 2019, S. 3). Die Ausweitung der Definition nach Schär und Stanoevska-Slabeva wird in dieser Arbeit als Definition von Digital Nudging definiert.

Neben der Gestaltungsfreiheit in der digitalen Sphäre können Entscheidungsarchitekten auch von Daten profitieren, die durch Anwender/innen generiert werden: Aus diesem Wissen können Erkenntnisse zu ihren Verhaltensweisen abgeleitet werden, um Nudges noch effektiver zu gestalten. Es ist sogar denkbar, dass durch die Information, die der/die Nutzer/in preisgibt, ein Nudge individuell auf sie oder ihn abgestimmt werden kann (Schneider, 2019, S. 73).

Die Nutzung von Digital Nudges ist vielfältig und wird aufgrund der Zunahme an digitalen Angeboten laufend relevanter. Da soziale Netzwerke nur in digitaler Form existieren, werden im Rahmen der vorliegenden Arbeit die Anwendung und die Effektivität des Digital Nudgings analysiert. Dabei soll eine spezielle Art des (Digital) Nudgings im Detail geprüft werden: Dieser sogenannte Social-Norm-Nudge wird im nachfolgenden Kapitel betrachtet.

5 Soziale Normen

Als letzter Bestandteil des Forschungsstands werden die sozialen Normen genauer betrachtet, den mit sozialen Normen arbeitet der Social-Norm-Digital-Nudge. Daher wird in diesem Kapitel soziale Normen erläutert. Folglich die Anwendung in Form eines Nudges genauer betrachtet.

5.1 Überblick

Soziale Normen bilden Standards und Regeln, die von einer Gruppe akzeptiert beziehungsweise nicht akzeptiert und somit als normal angesehen werden (Stok & de Ridder, 2019, S. 95). Es gibt zwei Arten von sozialen Normen: In deskriptiven Normen wird beschrieben, was eine bestimmte Mehrheit von Personen macht oder auch nicht macht. In Kontrast dazu wird in induktiven Normen festgehalten, was durch eine bestimmte Mehrheit von Personen als akzeptiert oder nicht akzeptiert erachtet wird (Cialdini, Kallgren & Reno, 1991, S. 202–203).

Als soziales Wesen passt sich der Mensch häufig an das Verhalten anderer Menschengruppen an – dies bestätigt Asch (1955) in seiner Untersuchung. Er befasste sich damit, ob sich einzelne Personen einer eindeutig falschen Antwort einer Gruppe anpassen oder diese korrigieren. Im Ergebnis übernahmen viele die falsche Antwort, unabhängig davon, wie eindeutig falsch diese war. Der Mensch passt sein Verhalten somit an das der Gruppe an. Dies passiert unbewusst und ohne aktives Handeln (Chartrand & Bargh, 1999, S. 900).

Die Tatsache, dass sich Menschen an Gruppen orientieren, haben auch Thaler und Sunstein (2009) erkannt. Sie wenden die Erkenntnisse der Gruppenkonformität und zu den sozialen Normen in der Nudging-Theorie an.

5.2 Social-Norm-Nudge

Mit dem Social-Norm-Nudge wird versucht, Personen mitzuteilen, was eine Mehrheit tun würden, um das Verhalten des/der Einzelnen zu ändern (Thaler & Sunstein, 2009). Diese Form zählt zu den effektivsten Nudges (Sunstein, 2014, S. 58), was sich auch in einem Experiment zeigte, in dem versucht wurde, Personen davon zu überzeugen, mehr erneuerbare Energie in ihre Stromversorgung zu integrieren: Dabei war der Social-Norm-Nudge neben dem Default-Nudge am effektivsten (Momsen & Stoerk, 2014, S. 380). Ebenfalls konnten Gonçalves, Coelho, Martinez und Monteiro (2021) eine signifikante Wirkung eines Social-Norm-Nudges nachweisen. Mit dem Social-Norm-Nudge der im

Einkaufswagen platziert wurde: «die gesündesten Familien dieses Supermarktes kaufen mindestens elf Früchte und Gemüse pro Einkauf und Sie?» (Gonçalves et al., 2021, S. 6), versuchten sie, Personen dazu zu bringen, in einem Supermarkt mehr Obst und Gemüse zu kaufen. Über drei Monate konnte bei den Probandinnen und den Probanden ein Anstieg von 25% in der gekauften Menge an Obst und Gemüse festgestellt werden. Folglich konnte die einfache Platzierung eines Social-Norm-Nudges im Einkaufswagen Personen dazu motivieren, mehr Obst und Gemüse zu kaufen (Gonçalves et al., 2021).

6 Hypothesen

Um die Forschungsfrage vollumfänglich zu beantworten, wurden sieben Hypothesen abgeleitet, die im Rahmen der vorliegenden Bachelorarbeit überprüft werden sollen. Sie basieren auf den Erkenntnissen der Forschung und werden in diesem Kapitel erläutert. Anhand des in den vorangehenden Kapiteln erarbeiteten Forschungsstands konnte festgestellt werden, dass ein Social-Norm-Nudge eine effektive Form des Nudgings bildet. Daraus ergibt sich die Frage, ob ein solcher Nudge auch zur Erhöhung der Sicherheitssensibilität in sozialen Netzwerken führen könnte. Dazu wurden folgende Hypothesen aufgestellt:

6.1 Ableitung

Die erste Hypothese bezieht sich darauf, ob die Wirkung eines Social-Norm-Digital-Nudges auf das Selbstoffenbarungsverhalten beziehungsweise die Einstellungen der Teilungsoptionen einen signifikanten Einfluss nimmt. Es wird vermutet, dass Personen, die einen Social-Norm-Digital-Nudge sehen, der dazu animiert, eine restriktivere Teilungseinstellung vorzunehmen, dazu neigen, diesem Anstoss zu folgen. Mehrere Studien zeigen, dass andere Personen(gruppen) Einfluss auf das eigene Verhalten ausüben (Acquisti et al., 2012; Asch, 1955; Barak & Gluck-Ofri, 2007; Lee et al., 2020; Taddicken, 2014). Die Vermutung liegt somit nahe, dass mithilfe eines Social-Norm-Digital-Nudges, der ebenfalls auf dem sozialen Einfluss basiert, die Selbstoffenbarung verringert werden könnte. Die allgemeine Wirkung eines solchen Nudges auf das Verhalten konnte in den Experimenten von Gonçalves et al. (2021) sowie Momsen und Stoerk (2014) nachgewiesen werden. Daher wird folgende Hypothese aufgestellt:

H1: Personen, die einen Social-Norm-Digital-Nudge bei der Einstellung der Teilungsoptionen erhalten, weisen im Durchschnitt eine niedrigere Selbstoffenbarung auf als diejenigen, die keinen Nudge erhalten.

Neben der Bestätigung dieser Annahme soll in der vorliegenden Arbeit auch das Erforschen der Wirkung eines Nudges untersucht werden. Eine Vermutung besteht darin, dass das Risikobewusstsein keinen Einfluss auf die Wirkung eines Social-Norm-Digital-Nudges sowie die Selbstoffenbarung nimmt. Ein Zusammenhang zwischen der Selbstoffenbarung und dem Risikobewusstsein konnte bereits in anderen Untersuchungen ausgeschlossen werden (Cheung et al., 2015; Taddicken, 2014). Zudem werden die Hypothesen H2a und H2b gestützt von der Privacy-Paradox-Theorie, die besagt, dass Personen ihre Daten unabhängig von Risikobedenken preisgeben (Gerber et al., 2017,

S. 142), was auf das Fehlen eines Effektes des Risikobewusstseins auf die Selbstoffenbarung hindeutet. Zudem haben Bernath et al. (2020, S. 62–63) in ihrer zweijährlichen Studie zur Mediennutzung von Jugendlichen festgestellt, dass zwei Drittel dieser ihre Privatsphäre aktiv schützen, obwohl nur etwa ein Drittel sich Sorgen macht bezüglich der Sichtbarkeit von persönlichen Inhalten. Das zeigt, dass das Risikobewusstsein nicht direkt mit der Selbstoffenbarung zusammenhängt. Zusätzlich kamen in den Jahren 2016 bis 2018 vermehrt Datenschutzmissbräuche von Facebook an die Öffentlichkeit (Betschon, 2018). Nichtsdestotrotz stiegen die Nutzerzahlen des Netzwerks (Facebook Inc., 2021), was auf ein fehlendes Risikobewusstsein von Nutzenden hindeutet. Zusammengefasst wird in dieser Arbeit davon ausgegangen, dass das Risikobewusstsein keinen Einfluss auf die Wirkung des Social-Norm-Digital-Nudges sowie darauf ausübt, ob Personen Inhalte teilen. Daher werden folgende Hypothesen aufgestellt:

H2a: Das Risikobewusstsein hat keinen Effekt auf die Wirkung des Social-Norm-Digital-Nudges auf die Selbstoffenbarung.

H2b: Das Risikobewusstsein hat keinen Effekt auf die Selbstoffenbarung.

Einen möglichen Einfluss auf die Wirkung könnte das Bedürfnis nach Popularität haben, denn ein verstärkender Effekt auf die Selbstoffenbarung konnte für sie bereits in mehreren Studien nachgewiesen werden (Cheung et al., 2015; Christofides et al., 2009; Hallam & Zanella, 2017; Hollenbaugh & Ferris, 2014; Ng, 2014; Utz et al., 2012). Teilweise wird sie sogar als grösster Einflussfaktor der Selbstoffenbarung eingeschätzt (Cheung et al., 2015; Hallam & Zanella, 2017). Das bedeutet, dass Personen, die ein hohes Bedürfnis nach Popularität haben, dazu neigen, viel zu teilen. Christofides et al. (2009) vermuten, dass sogar Facebook bewusst denjenigen Personen mehr Reichweite gibt, die viel teilen. In neueren sozialen Netzwerken ist es bekannt, dass entsprechend vorgegangen wird (Bernath et al., 2020, S. 62–63). Nun stellt sich die Frage, ob das Bedürfnis nach Popularität die Wirkung eines Social-Norm-Digital-Nudges verstärkt oder verschlechtert. Aufgrund der genannten Erkenntnisse kann davon ausgegangen werden, dass Bedürfnis nach Popularität sich negativ auf die Wirkung des Nudges auswirkt. Wie Christofides et al. (2009) annehmen, hätte die organische Reichweite beim manuellen Einschränken durch den Algorithmus starke negativen Folgen, die einer Person zu hohe Opportunitätskosten verursachen könnte – unabhängig davon, ob ein Nudge vorhanden ist. Auf diesem Zusammenhang basierend wird in Hypothese 3b ein positiver Effekt des Bedürfnisses nach Popularität auf die Selbstoffenbarung angenommen. Wenn ihr Bedürfnis nach Popularität hoch ist, teilt die Person somit viele persönlichen Informationen über ihr Leben. Daher werden folgende Hypothesen aufgestellt.

H3a: Das Bedürfnis nach Popularität schwächt die Wirkung des Social-Norm-Digital-Nudges auf die Selbstoffenbarung.

H3b: Das Bedürfnis nach Popularität hat einen positiven Effekt auf die Selbstoffenbarung.

Die Wirkung der Gruppenkonformität auf das eigene Verhalten konnte bereits bestätigt werden (Acquisti et al., 2012; Asch, 1955; Barak & Gluck-Ofri, 2007; Lee et al., 2020; Taddicken, 2014). In sozialen Netzwerken ist eine Person kontinuierlich in Kontakt mit geteilten persönlichen Informationen anderer Nutzer und Nutzerinnen (Abramova et al., 2017, S. 7). Menschen, die eine hohe Gruppenkonformität aufweisen, könnten dazu neigen, generell ähnliche Inhalte zu veröffentlichen. Darum wird vermutet, dass die Gruppenkonformität einen positiven Effekt auf die Selbstoffenbarung hat. Auch wird angenommen, dass sie sich verstärkend auf die Wirkung eines Social-Norm-Nudges auswirkt. Ein Social-Norm-Digital-Nudge basiert auf sozialen Normen, d. h. nicht ausgesprochenen Regeln einer Gruppe, die eingehalten werden müssen, um von dieser akzeptiert zu werden (Stok & de Ridder, 2019, S. 95). Die Vermutung liegt daher nahe, dass die Gruppenkonformität einen verstärkenden Effekt auf die Wirkung eines Social-Norm-Digital-Nudges hat. Folgende Hypothesen werden aufgrund dessen aufgestellt:

H4a: Die Gruppenkonformität verstärkt die Wirkung des Social-Norm-Digital-Nudges auf das Selbstoffenbarungsverhalten.

H4b: Die Gruppenkonformität hat einen positiven Effekt auf die Selbstoffenbarung.

Zur Veranschaulichung der obigen Annahmen wurde ein Hypothesenmodell erstellt. Es zeigt die verschiedenen Variablen und deren Wirkung beziehungsweise Einfluss untereinander. Die durchgezogenen Linien stehen für Hypothesen, in denen ein Zusammenhang beziehungsweise eine Wirkung kommuniziert wird. Die gestrichelten Linien zeigen Hypothesen, in denen keine Wirkung vermutet wird.

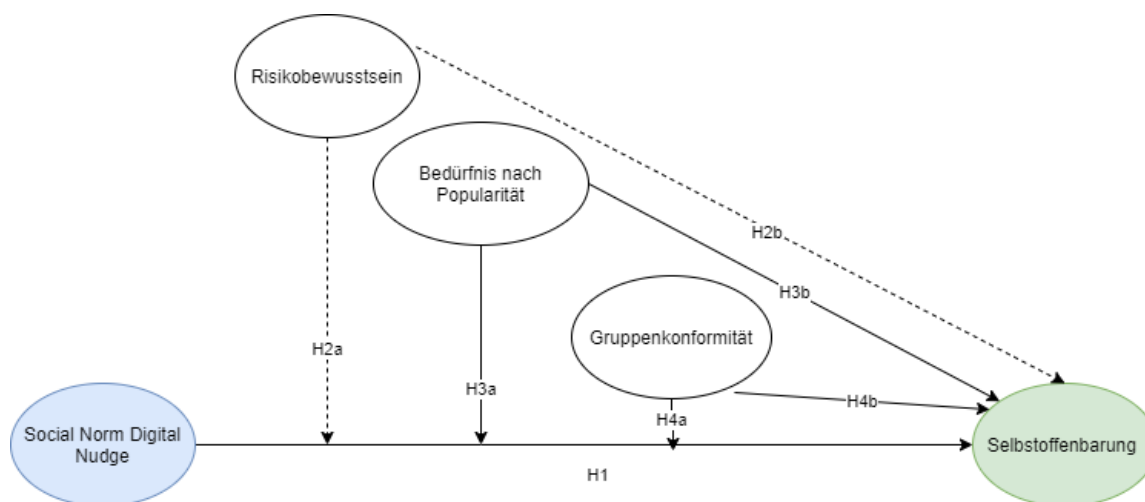


Abbildung 3: Hypothesenmodell.
Quelle: eigene Darstellung

6.2 Operationalisierung

In den sieben Hypothesen, die in Kapitel 6 bislang vorgestellt wurden, sind fünf verschiedene Variablen relevant: Social-Norm-Digital-Nudge (H1, H2a, H3a, H4a), das Selbstoffenbarung (H1, H2a, H2b, H3a, H3b, H4a, H4b), das Risikobewusstsein (H2a, H2b), das Bedürfnis nach Popularität (H3a, H3b) und die Gruppenkonformität (H4a, H4b). Zum Einordnen ihrer Wirkung wurden anhand der Theorie Messkonstruktionen erstellt, auf die in diesem Kapitel eingegangen wird.

In der Arbeit von Díaz Ferreyra, Meis und Heisel (2017) wurden neun Dimensionen und 30 Attribute der Selbstoffenbarung definiert. Es wurden zwölf Attribute zur Messung von sieben Dimensionen ausgewählt, damit die Anzahl der Umfragefragen nicht zu hoch ist und Ermüdungseffekte entstehen. In der Auswahl wurde darauf geachtet, dass die Attribute möglichst verschiedene Intimitätsgrade aufwiesen. Zur Auswahl wurden Angaben aus Profilinformatoren, die auf Facebook oder Bumble angegeben werden können, mit den Attributen von Díaz Ferreyra et al. (2017) verglichen. Dabei wurden hauptsächlich Informationen beachtet, die typischerweise bei Anmeldungen beziehungsweise bei der Profilerstellung erfasst werden können. Diesen Angaben wurden drei weitere Attribute hinzugefügt, die nicht im Profil zu finden sind – Krankheiten, die Telefonnummer und die Wohnadresse. Der Wohnort kann in sozialen Netzwerken zwar genannt werden, allerdings ist mit der Wohnadresse in dieser Arbeit die gesamte Adresse inklusive Strasse gemeint.

Die Variable wird anhand einer ordinalen Skala gemessen. So können Testpersonen pro Attribut jeweils aus einer fünfstufigen Skala auswählen, mit wem die genannte Information geteilt werden sollte (nur ich, enge Freundinnen und Freunde, Freundinnen und

Freunde, Freundinnen und Freunde von Freunden, jeder). Die Werte werden pseudometrisch ausgewertet. Dazu werden die Skalenwerte jedes Attributs ohne Gewichtung zu einer Summe addiert. Diese ergibt die Variable ‹Selbstoffenbarung›. Je höher der Wert dieser Variablen ist, desto intensiver fällt die Selbstoffenbarung aus.

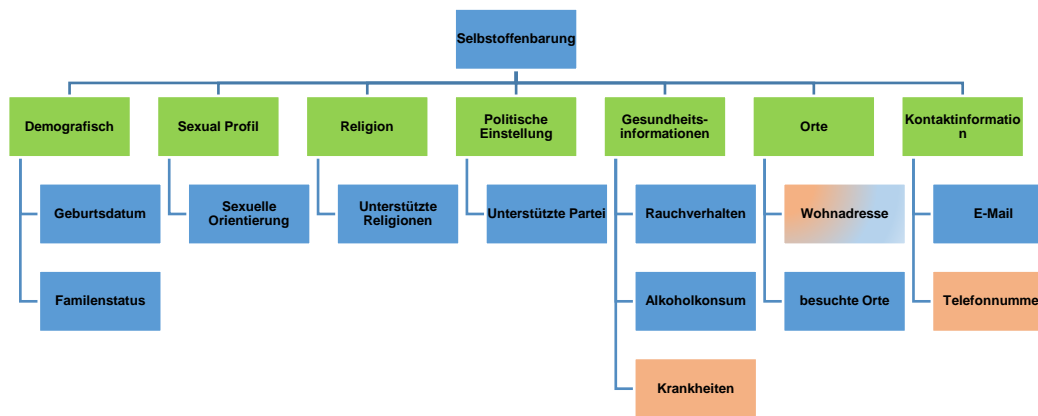


Abbildung 4: Dimensionen und Attribute der Variablen ‹Selbstoffenbarung›.

Quelle: eigene Darstellung in Anlehnung an Diaz Ferreyra et al. (2017).

Die Variable ‹Social-Norm-Digital-Nudge› ist ein nominales Mass. Sie wird benötigt, um in Gruppen einzuteilen und folglich zu messen, welchen Einfluss das Vorhandensein eines ‹Social-Norm-Digital-Nudge› auf andere Variablen aufweist. Die Variable variiert zwischen ‹vorhanden› und ‹nicht vorhanden›.

Die Variable ‹Risikobewusstsein› wird mit verschiedenen Items gemessen. Es wird versucht, das Risikobewusstsein der sozialen Privatsphäre zu erfassen. Die acht hierzu genutzten Items wurden verschiedenen wissenschaftlichen Arbeiten entnommen (Krasnova, Spiekermann, Koroleva & Hildebrand, 2010; Malhotra, Kim & Agarwal, 2004; Taddicken, 2014). Ihre Messung erfolgt auf einer ordinalen Skala, deren Werte ähnlich wie bei der Variablen ‹Selbstoffenbarung› summiert und zu einem Wert zusammengefasst werden. Letzterer Wert entspricht der Variablen ‹Risikobewusstsein›. Der Wert kann von acht bis maximal 40 reichen. Je höher er ist, umso höher ist das Risikobewusstsein der Person. Der Cronbachs Alpha wird bei der Auswertung des Experiments sowie beim Auswerten des Pretests ebenfalls gemessen.

Item	Item-Text
RBS01	Insgesamt sehe ich eine echte Gefährdung meiner Privatsphäre durch meine Präsenz auf sozialen Netzwerken.
RBS02	Ich befürchte, dass mir aufgrund meiner Präsenz auf sozialen Netzwerken etwas Schlimmes passieren könnte.
RBS03	Ich fühle mich nicht sicher bei der Veröffentlichung meiner persönlichen Daten auf sozialen Netzwerken.
RBS04	Ich bin besorgt über einen möglichen Online-Identitätsdiebstahl.
RBS05	Ich bin besorgt darüber, dass sich meine Follower als jemand anders ausgeben.
RBS06	Ich bin besorgt darüber, dass Personen, die ich nicht kenne, persönliche Informationen über mich sehen.
RBS07	Insgesamt finde ich es riskant, meine persönlichen Daten auf sozialen Netzwerken zu veröffentlichen.
RBS08	Bitte bewerten Sie, wie Sie das Risiko für Ihre Privatsphäre bei der Nutzung von sozialen Netzwerken insgesamt einschätzen.

Tabelle 1: Items der Variablen «Risikobewusstsein».

Quelle: eigene Darstellung in Anlehnung an Krasnova, Spiekermann, Koroleva & Hildebrand, 2010; Malhotra, Kim & Agarwal, 2004; Taddicken, 2014.

Die Variable «Bedürfnis nach Popularität» wird ebenfalls auf einer ordinalen Skala gemessen. Dabei werden die Items aus einer Befragung von Santor, Messervey und Kusumakar (2000) an Schulkindern einer US-amerikanischen High School als Ausgangspunkt herangezogen. Mit Anpassungen sollen die Items so gestaltet und teilweise ergänzt werden, dass sie auch von Erwachsenen ausgefüllt werden können. Auf der genutzten Skala soll das Gefühl beziehungsweise der Druck gemessen werden, aufgrund der Popularität etwas zu tun, was andernfalls nicht gemacht werden würde (Santor et al., 2000, S. 166). Die Summe der pseudometrischen Auswertung ergibt die Variable «Bedürfnis nach Popularität» und kann einen Wert von zwölf bis 60 annehmen. Je höher der Wert liegt, umso stärker ist das Bedürfnis, populär zu sein.

Item	Item-Text
BNP01	Ich habe schon Dinge getan, die ich sonst nicht mache, um mich beliebter zu machen.
BNP02	Ich habe schon Freunde vernachlässigt aufgrund dessen, was andere denken könnten.
BNP03	Ich mache fast alles, um nicht als Versager angesehen zu werden.
BNP04	Es ist mir wichtig, dass andere denken, dass ich beliebt bin.
BNP05	Manchmal verbringe ich Zeit mit Personen, nur weil diese beliebt sind.
BNP06	Ich habe schon Sachen gekauft, nur weil sie im Trend waren.
BNP07	Teilweise wechsele ich die Art, mich zu kleiden, um beliebter zu sein.
BNP08	Ich bin schon mit jemandem befreundet gewesen, nur weil andere Personen diese Person mögen.
BNP09	Ich bin schon auf Partys gegangen, nur um Teil der Menge zu sein.
BNP10	Ich mache oft Dinge, nur um bei Menschen beliebt zu sein.
BNP11	Manchmal bin ich mit Leuten unterwegs, damit andere nicht denken, ich sei unbeliebt.
BNP12	Ich habe Angst, von anderen als unbeliebt wahrgenommen zu werden.

Tabelle 2: Items der Variablen «Bedürfnis nach Popularität».

Quelle: eigene Darstellung in Anlehnung an Santor, Messervey & Kusumakar, 2000.

Die Variable «Gruppenkonformität» wird auf einer ordinalen Skala gemessen. Sie wurde aus zwei Konstrukten von Stibe und Cugelman (2019) übernommen. Die Gruppenkonformität wird in dieser Arbeit anhand Konstrukte aus sozialen Normen und dem sozialen Vergleich gemessen. Dabei wird anhand der sozialen Normen erfasst, einen wie starken Einfluss das Verhalten einer anderen Person auf das eigene Verhalten hat. Hingegen wird im sozialen Vergleich erfasst, wie sich eine Person an einer anderen Person orientiert. Anhand dieser Konstrukte wurde eine Skala entworfen, die die Gruppenkonformität messen soll.

Item	Item-Text
GKN01	Ich vergleiche mich mit anderen Personen.
GKN02	Ich vergleiche häufig, wie es mir im Vergleich zu anderen Personen geht.
GKN03	Ich bewerte meine Leistung im Vergleich zu anderen.
GKN04	Ich ziehe es vor, das zu tun, was andere Personen normalerweise tun.
GKN05	Ich ziehe es vor, so zu handeln, wie alle anderen handeln.
GKN06	Ich befolge Verhaltensweisen, die Menschen typischerweise tun.
GKN01	Ich vergleiche mich mit anderen Personen.
GKN02	Ich vergleiche häufig, wie es mir im Vergleich zu anderen Personen geht.

Tabelle 3: Items der Variablen <Gruppenkonformität>.

Quelle: eigene Darstellung in Anlehnung an Krasnova, Spiekermann, Koroleva & Hildebrand, 2010; Malhotra, Kim & Agarwal, 2004; Taddicken, 2014.

7 Methodik

Durch eine experimentelle Befragung sollte im Rahmen der vorliegenden Arbeit herausgefunden werden, ob die Testpersonen ihre Wahl der Zielgruppe, mit der sie Inhalte teilen, ändern, wenn sie in ihrer Entscheidung durch Social-Norm-Digital-Nudges unterstützt werden. Den Teilnehmenden wurden zudem am Schluss der Befragung Fragen gestellt, mit denen die Variablen ‹Gruppenkonformität›, ‹Bedürfnis nach Popularität› und ‹Risikobewusstsein› gemessen werden sollten. Dadurch sollten Anhaltspunkte zum Einfluss der verschiedenen Variablen auf das Selbstoffenbarungsverhalten in sozialen Netzwerken gesammelt werden. Vor dem Einsatz dieser Fragen erfolgte das eigentliche Experiment, in deren Rahmen das von der Hochschule bereitgestellte Umfragetool LimeSurvey verwendet wurde.

7.1 Erhebungsdesign

Das Experiment wurde in einem einfaktoriellen Between-Subject-Design durchgeführt. Dabei wurde die Variable ‹Social-Norm-Digital-Nudge› zwischen ‹vorhanden› und ‹nicht vorhanden› variiert. Es wurde mit Vignetten gearbeitet. So sollten die Befragten keine klassischen Fragen erhalten, sondern es wurden Situationsbeschreibungen verwendet, um ein mögliches Szenario abzubilden (Ausprung, Hinz & Liebig, 2009, S. 59). Vignetten gelten als innovative Methode der Sozialforschung und eignen sich vor allem zur Norm- und Einstellungsforschung. Zu beachten ist jedoch, dass die Komplexität der Vignetten einen signifikanten Einfluss auf die Befragungsergebnisse aufweist (Ausprung et al., 2009, S. 87). Nichtsdestotrotz werden Vignetten als für diese Untersuchung geeignete Methode erachtet, da bei der Messung des Einflusses eines Social-Norm-Nudges eine möglichst realitätsnahe Situation geschaffen werden soll. Durch die Beschreibung der Szenarien konnten sich die Testpersonen in diese hineinversetzen und dadurch ehrliche Antworten geben. Sie wurden zufällig in zwei Gruppen eingeteilt. Die experimentelle Gruppe erhielt den Social-Norm-Digital-Nudge, die Kontrollgruppe sah keinen Social-Norm-Digital-Nudge. Es wurden maximal zwölf Vignetten erstellt. Die Vignetten enthielten jeweils ein Szenario, in dem zu entscheiden war, mit wem eine bestimmte Information geteilt werden sollte. Die Personen, die der Experimentalgruppe zugeordnet wurden, sahen die Eingabemaske von Facebook mit einem auffallenden Social-Norm-Digital-Nudge, der eine deskriptive Norm beinhaltete und darauf hinwies, dass die Mehrheit der Personen auf Facebook diese Information nur mit einer bestimmten Zielgruppe teilt. Beispielsweise sah ein Nudge so aus: ‹Die meisten Personen teilen diese Information nur mit Freundinnen und Freunden›. Mit verschiedenen Vignetten wurde versucht, verschiedene

Dimensionen der Selbstoffenbarung abzudecken. So sollten Informationen mit hoher bis niedriger Intimität abgefragt werden.

Die Probanden und die Probandinnen sahen eine Vignette, in deren Rahmen sie sich auf Facebook registrieren und entscheiden mussten, mit wem welche Informationen geteilt werden sollten. Die Vignette wurde mit variierenden Profilinformationen eingesetzt. Folgende Beschreibung wurden in der Umfrage verwendet (siehe auch Anhang II):

Stellen Sie sich bitte vor, dass Sie auf Facebook einen neuen Account erstellen. Dort müssen Sie zwölf persönliche Informationen angeben. (erstes Item – Beschreibung)

Sie sind nun dabei, auszuwählen, mit wem Sie Ihr Geburtsdatum teilen möchten. Welche Option würden Sie wählen? (Beschreibung der darauffolgenden Items)

Zur Unterstützung wurde ein Bild der Eingabemaske von Facebook zur Verfügung gestellt. Diese wurden vom sozialen Netzwerk übernommen und teilweise mit einem Fotoeditor bearbeitet. Die Teilungsoptionen wurden wegen eines möglichen Response-Sets zufällig pro Frage neu angeordnet. Die Optionen im Nudge wurden zwischen «nur ich», «enge Freundinnen und Freunde» sowie «Freundinnen und Freunde» variiert, um ihre Glaubwürdigkeit sicherzustellen. Ferner wurde bei einigen Angaben darauf verzichtet, eine Information im Voraus auszufüllen, um zu vermeiden, dass Personen ihre Wahl aufgrund ihrer Zuneigung oder Abneigung gegenüber der Information treffen. Alle Nudges sind im Anhang enthalten (siehe Anhang I).

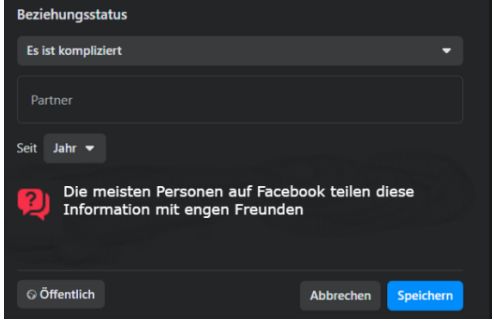
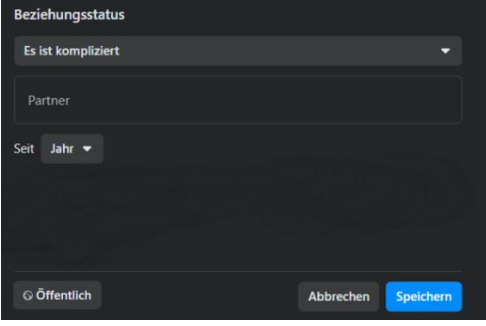
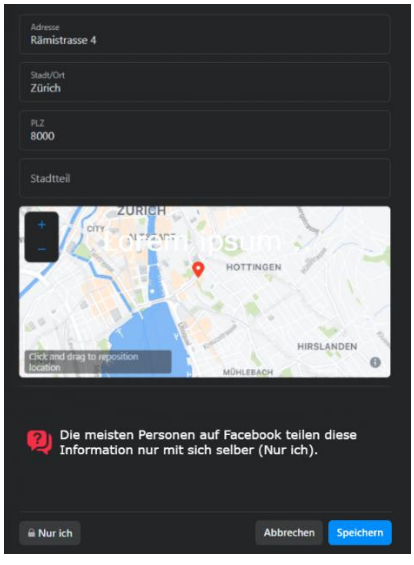
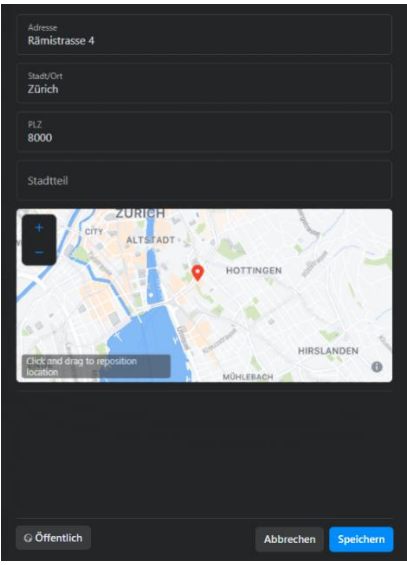

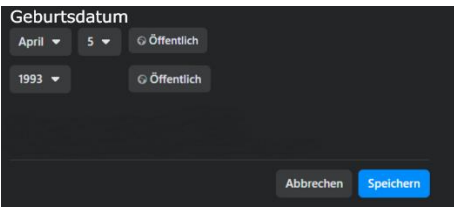
Nudge vorhanden	Nudge nicht vorhanden
	
	
	

Tabelle 4: Nudges im einfaktoriellen Forschungsdesign

Quelle: eigene Darstellung. Anmerkung: Eingabemasken wurden von Facebook übernommen und angepasst. Die restlichen Nudges sind im Anhang I einsehbar.

Nach dem beschriebenen Experiment wurden auch zahlreiche Fragen gestellt. Darunter waren Fragen zur Nutzung der sozialen Netzwerke bzw. zu Erfahrungen mit Risiken, aber auch soziodemografische Fragen enthalten. Diese zusätzlichen Angaben wurden aufgrund ihrer eventuellen Nützlichkeit für die Auswertung erhoben, sie sollten bei der Interpretation helfen.

7.2 Pretest und Stichprobenerhebung

Die Grundgesamtheit der Umfrage beinhaltet alle Personen in der Schweiz (Stand 2020: 8'667'100), die als ihre Hauptsprache Deutsch oder Schweizerdeutsch beherrschen

(62,1%) (Bundesamt für Statistik, o. D.-b). Dementsprechend besteht die Grundgesamtheit aus ungefähr 5.382 Millionen Menschen. Damit die Resultate möglichst repräsentativ gegenüber der Grundgesamtheit sind, wurde eine Stichprobengröße von 385 Personen bei einem Konfidenzintervall von 95% und einer Fehlerspanne von 5% mithilfe des Stichprobenrechners von SurveyMonkey berechnet (SurveyMonkey, o. D.-b).

Damit in der tatsächlichen Befragung keine unvorhergesehenen Fehler passieren, wurden das erstellte Experiment und der Fragebogen getestet. Dazu wurde während drei Tagen ein Pretest durchgeführt. Insgesamt konnte 25 Teilnehmende gefunden werden, die die Umfrage testweise ausfüllten und ein Feedback zu ihr gaben. Angemerkt wurden in erster Linie kleine Fehler wie Rechtschreib- oder Formulierungsfehler, die korrigiert wurden. Zusätzlich wurde mit den gesammelten Daten versucht, die geplanten Auswertungen durchzuführen. Dabei wurde auch das Cronbachs Alpha der verschiedenen Skalen im Fragebogen errechnet. Alle Skalen ergaben mindestens einen akzeptablen Wert hierfür (Risikobewusstsein: neun Items; $\alpha = .800$, Gruppenkonformität: sechs Items; $\alpha = .828$, Bedürfnis nach Popularität: zwölf Items; $\alpha = .786$) im Pretest, daher wurde die Umfrage im Weiteren versendet.

Bei der Erhebung der Stichprobe wurde bewusst auf die Verwendung von bezahlten Antworten verzichtet, da das Netzwerk des Verfassers bereits ungefähr 350 Kontakte enthielt. Hätten diese Kontakte die Befragung jeweils an mindestens drei weitere Personen weitergeleitet, wären theoretisch 1400 Teilnehmende erreichbar gewesen. Es wurde allerdings berücksichtigt, dass nur eine Minderheit der Personen, die eine Umfrage als Weiterleitung erhält, diese tatsächlich ausfüllt. Nichtsdestotrotz war es wahrscheinlich, dass die benötigte Anzahl von 385 Personen mit dem eigenen Netzwerk erreicht werden können würde, was den Einsatz von bezahlten Antworten überflüssig machte.

7.3 Datenauswertung

Um die aufgestellten Hypothesen zu überprüfen, wurden die gesammelten Daten der Probanden mithilfe des Statistikprogramms IBM SPSS (Superior Performing Software System) ausgewertet. Dabei wurden zuerst alle Datensätze entfernt, die den Anforderungen nicht entsprachen. Antworten mit Unvollständigkeiten bezüglich der Fragen zur Erfassung der Selbstoffenbarung (mit den Nudges) wurden direkt in LimeSurvey aus dem Datensatz gestrichen. Die restlichen unvollständigen Antworten wurden im Datensatz behalten.

Im nächsten Schritt wurden die Fragen in SPSS importiert. Es wurden Merkmalsträger entfernt, die die Kontrollfrage nicht korrekt beantworteten, denn im Fragebogen war eine

Kontrollfrage platziert worden (siehe Anhang II – Frage KF01). In dieser wurden die Teilnehmenden der experimentellen Umfrage gebeten, bei einer Matrixfrage die Zahl vier auszuwählen. Mit dieser Kontrollfrage konnte überprüft werden, ob die Teilnehmenden die Fragen beziehungsweise die Items aufmerksam lasen oder sich nicht nur durchklickten. Beim Durchführen der Befragung wurde bemerkt, dass die Kontrollfrage nicht immer als solche identifiziert werden konnte. Daher haben sie einige ausgelassen, da sie sich nicht sicher waren, ob die Vier ausgewählt werden darf, da sich die Kontrollfrage zwischen den Fragen zu Items für die Messung des Bedürfnisses nach Popularität befand. Deshalb wurden nur Personen aus dem Datensatz entfernt, die eine Antwort gewählt haben, die nicht der Vier entsprach. Personen, die keine Antwort gaben, wurden im Datensatz behalten, da die Vermutung nahe liegt, dass diese nicht genau wussten, was sie auswählen sollten, und die Items wahrscheinlich aufmerksam gelesen haben.

Nach der Bereinigung des Datensatzes wurden aus den Daten Werte für die Variablen berechnet, um die Hypothesen prüfen zu können. Auch wurden die nötigen statistischen Verfahren wie die lineare Regression und der t-Test angewandt. Die detaillierten Berechnungen sowie die Auswertungen, die im Rahmen dieser Arbeit vorgenommen wurden, sind in der Syntax im Anhang (siehe Anhang III) enthalten.

8 Ergebnisse

Zwischen dem 28.07.2021 und dem 10.07.2021 wurde die Umfrage an Bekannte des Verfassers gesendet. Dazu wurde eine persönliche Nachricht auf WhatsApp, LinkedIn, Facebook oder Instagram genutzt. Die Umfrageteilnehmende wurden zudem dazu aufgefordert, die Umfrage in ihrem Bekanntenkreis mit mindestens drei Personen zu teilen. Damit nachverfolgt werden konnte, dass die Personen die Umfrage ausfüllten, wurde sie zudem gebeten, ein Daumenhoch-Emoji zurückzusenden, sofern dies erfolgt war. Dadurch wurde es ermöglicht, Erinnerungen an diejenigen zu senden, die das Ausfüllen vergessen hatten. Über entsprechende Erinnerungen konnten über 100 Antworten eingeholt werden. Ebenfalls wurde die Umfrage im Forum für Umfragen der Fachhochschule Graubünden geteilt und gegen Schluss des Befragungszeitraums wurden ein Post in den obengenannten sozialen Netzwerken verfasst sowie eine Antwort durch Pollpool erreicht. Dadurch konnten insgesamt 362 Teilnehmende für die Umfrage gefunden werden. Es wurden bereits während des Befragungszeitraums regelmässig Antwortende entfernt, die Fragen zur Selbstoffenbarung (Experiment) nicht vollständig ausgefüllt hatten.

8.1 Stichprobe

In diesem Unterkapitel werden die Merkmale der Stichprobe präsentiert. Nach dem Bereinigen des Datensatzes von 362 Teilnehmenden gemäss Kapitel 7.3 blieben noch 336 Antworten übrig, die für die Auswertung gültig sind. 26 Teilnehmende wurden aufgrund des Nichtbestehens der Kontrollfrage ausgeschlossen. Gemäss SurveyMonkey (o. D.-a) liegt bei einer Grundgesamtheit von 8,677 Millionen Personen, einem Konfidenzniveau von 95% und einer Stichprobengrösse von 326 Personen die Fehlerspanne bei 5%.

Nachfolgend wird auf die Zusammensetzung der Stichprobe eingegangen: Die Teilnehmenden waren zu 45.5% weiblich, zu 50% männlich und zu 0.6% divers. 3.9% der Teilnehmenden beantworteten die Frage zum Geschlecht nicht. Daher ist das Geschlecht ungefähr gleichmässig verteilt. Die Stichprobe ist eher jung, die befragten Personen befanden sich im Alter von 15 bis 70 Jahren. Das Durchschnittsalter der Teilnehmenden betrug 28.1 Jahre. Es fielen 50% der Teilnehmenden in die Altersspanne von 22 bis 29 Jahren. Am stärksten waren die Altersgruppen von 19 bis 24 bzw. von 25 bis 34 Jahren vertreten, gefolgt von den 45- bis 54-Jährigen. Das Bildungsniveau verteilte sich relativ ausgeglichen mit 28.5% der Befragten, die einen Bachelorabschluss einer Hochschule besaßen, 18.5%, die eine Berufslehre absolviert hatten, und 15.5% mit der Berufsmaturität. Zudem waren die meisten Personen in der Stichprobe erwerbstätig (72.6%). Darin wurden auch Studierende einberechnet, sofern diese neben ihrem Studium einer Er-

werbstätigkeit nachgingen. In der Stichprobe sind alle Ausprägungen der Merkmale mindestens einmal vorhanden, die Verteilung innerhalb der Merkmale ist allerdings nicht bei allen Merkmalen gleich gross. Woraus einen möglicher Einfluss auf die Ergebnis entstehen könnte.

Die Teilnehmenden der Umfrage wurden für das Experiment anhand des Zufallsgenerators von LimeSurvey in zwei Gruppen eingeteilt. Durch die Funktion rand(1,2) erhielt jede befragte Person zufällige eine Eins oder eine Zwei. Sofern den Teilnehmenden eine Eins zukam, wurden sie in die Experimentalgruppe eingeteilt, ansonsten in die Kontrollgruppe. Die Experimentalgruppe erhielt wie in Kapitel 7.1 erwähnt einen Nudge.

Um zu prüfen, ob die Gruppen in etwa gleich aufgestellt waren, wurden auch ihre demografischen Merkmale analysiert. Es konnte festgestellt werden, dass nur geringe Unterschiede bestanden, die auf die Zufallszuteilung zurückzuführen sind. Es gibt in keiner Gruppe gravierende Abweichungen der Anteile. Die genauen Werte der demografischen Merkmale sind in der untenstehenden Tabelle (siehe Tabelle 5) ersichtlich.

	Stichprobe		Experimentalgruppe		Kontrollgruppe	
Anzahl	336		171		165	
Geschlecht	Anzahl	%-Anteil	Anzahl	%-Anteil	Anzahl	%-Anteil
Keine Angabe	13	3.9	6	3.5	7	4.2
weiblich	153	45.5	75	43.9	78	47.3
männlich	168	50.0	90	52.6	78	47.3
divers	2	0.6	0	0	2	1.2
Durchschnittsalter	28.1		28.4		27.8	
Altersgruppen	Anzahl	%-Anteil	Anzahl	%-Anteil	Anzahl	%-Anteil
Keine Angabe	13	3.9	8	4.7	5	3.0
<= 18	19	5.	6	3.5	13	7.9
19–24	168	50.0	89	52.0	79	47.9
25–34	79	23.5	41	24.0	38	23.0
35–44	20	6.0	7	4.1	13	7.9
45–54	21	6.3	10	5.8	11	6.7
55–64	13	3.9	7	4.1	6	3.6
65+	3	0.9	3	1.8	0	0.0

Bildung	Anzahl	%-Anteil	Anzahl	%-Anteil	Anzahl	%-Anteil
Keine Angabe	12	3.6	7	4.1	5	3.0
obligatorische Schule	8	2.4	5	2.9	3	1.8
Berufslehre	62	18.5	34	19.9	28	17.0
Berufsmaturität	52	15.5	30	17.5	22	13.3
gymnasiale Maturität oder Fachmaturität	47	14.0	24	14.0	23	13.9
Bachelor (FH, Uni oder ETH)	96	28.6	41	24.0	55	33.3
Master (FH, Uni oder ETH)	26	7.7	13	7.6	13	7.9
Eidg. Diplom/Fachausweis	15	4.5	7	4.1	8	4.8
Diplom höhere Fachschule	18	5.4	10	5.8	8	4.8
Erwerbstätigkeit	Anzahl	%-Anteil	Anzahl	%-Anteil	Anzahl	%-Anteil
Keine Angabe	13	3.9	6	3.5	7	4.2
erwerbstätig	244	72.6	127	74.3	117	70.9
Mutterschafts-/Erziehungsurlaub oder Beurlaubung	1	0.3	1	0.6	0	0
in Ausbildung/Umbildung	23	6.8	9	5.3	14	8.5
nicht erwerbstätig/pensioniert	55	16.4	28	16.4	27	16.4

Tabelle 5: Demografische Merkmale der Stichprobe der Experimental- und der Kontrollgruppe
Quelle: eigene Darstellung.

8.2 Wirkung des Nudges auf die Selbstoffenbarung (Hypothese 1)

H1: Personen, die einen Social-Norm-Digital-Nudge bei der Einstellung der Teilungsoptionen erhalten, weisen im Durchschnitt eine niedrigere Selbstoffenbarung auf als diejenigen, die keinen Nudge erhalten

Die erste Hypothese bezieht sich auf die Wirkung eines Social-Norm-Digital-Nudges auf die Selbstoffenbarung, zu der ein Experiment erfolgte. Es wurden zwölf Versuche inkludiert. Würden alle Optionen des Nudges befolgt werden, würde in ihrem Ergebnis ein Selbstoffenbarungswert von elf resultieren. In sechs von zwölf Versuchen konnte der Social-Norm-Digital-Nudge Personen dazu bringen, die von Nudges gewollten Möglichkeiten zu wählen. In zwei Fällen entschied die Gruppe mit dem Nudge mehrheitlich über eine kleinere Zielgruppe. In den restlichen vier Fällen hat die Experimentalgruppe jeweils eine grössere Zielgruppe selektiert. Die Attribute mit der stärksten Wirkung sind das

Rauchen, die Partei und die E-Mail. Insgesamt wurden die mit dem Nudge unterstützten Optionen 6.2% häufiger selektiert als in der Kontrollgruppe. Letztere hat wiederum 6.6% häufiger eine niedrigere Zielgruppe ausgewählt.

Attribute (Option vom Nudge)	Restriktiver als der Nudge [%]	Option des Nudges [%]	Offener als der Nudge [%]
Alter (Freunde)	-2.8	+1.3	+1.5
Probanden mit Nudge	44.4	46.8	8.8
Probanden ohne Nudge	47.3	45.5	7.3
Beziehungsstatus (enge Freunde)	-1.8	0.0	+1.8
Probanden mit Nudge	51.5	15.8	32.7
Probanden ohne Nudge	53.3	15.8	30.9
Sexuelle Orientierung (enge Freunde)	+4.9	-2.7	-2.3
Probanden mit Nudge	64.3	5.8	29.8
Probanden ohne Nudge	59.4	8.5	32.1
Religion (nur ich)		+3.0	-3.0
Probanden mit Nudge		67.8	32.2
Probanden ohne Nudge		64.8	35.2
Partei (enge Freunde)	-8.3	+3.8	+4.5
Probanden mit Nudge	60.8	10.5	28.7
Probanden ohne Nudge	69.1	6.7	24.2
Rauchen (Freunde)	-3.3	+5.4	-2.
Probanden mit Nudge	73.1	17.5	9.4
Probanden ohne Nudge	76.4	12.1	11.5
Alkohol (Freunde)	3.1	-3.0	-0.1
Probanden mit Nudge	80.7	14	5.3
Probanden ohne Nudge	77.6	17	5.4
Krankheiten (nur ich)		-2.6	+2.6
Probanden mit Nudge		88.9	11.1
Probanden ohne Nudge		91.5	8.5
Heimadresse (nur ich)		-1.1	1.1
Probanden mit Nudge		81.9	18.1

Probanden ohne Nudge		83.0	17.0
Besuchte Orte (Freunde)	+1.5	-2.4	+0.9
Probanden mit Nudge	40.9	50.9	8.2
Probanden ohne Nudge	39.4	53.3	7.3
E-Mail-Adresse (nur ich)		3.7	-3.7
Probanden mit Nudge		64.9	35.1
Probanden ohne Nudge		61.2	38.8
Telefonnummer (nur ich)		0.8	-0.8
Probanden mit Nudge		77.8	22.2
Probanden ohne Nudge		77.0	23.0
Summe der Differenzen	-6.6	6.2	0.4

Tabelle 6: Unterschiede in der Wahl der Teilen Option zwischen Experimental- und Kontrollgruppe
 Quelle: eigene Darstellung. Bemerkung: Die Experimentalgruppe wird hier mit der Kontrollgruppe verglichen. Dabei stellt ein positiver Wert eine häufigere Auswahl der Option bei der Experimentalgruppe dar und ein negativer Wert eine häufigere Wahl bei der Kontrollgruppe.

Für die Auswertung der Hypothese wurden die Summe aller pseudometrischen Werte der Nudge summiert. Ein hoher Wert gibt eine starke Selbstoffenbarung zu erkennen, ein geringer eine niedrige. Nachfolgend werden die Mittelwerte der beiden Gruppen verglichen- In diesen Werten bestehen kaum Unterschiede: Der Mittelwert der Experimentalgruppe ($M = 9.13$, $SD = 7.201$, $n = 171$) liegt etwas tiefer als derjenige der Kontrollgruppe ($M = 9.12$, $SD = 7.179$, $n = 165$). In der ersten Hypothese wird angenommen dass es einen signifikanten Unterschied in der Selbstoffenbarung der Experimental- und der Kontrollgruppe gibt. Um dies zu überprüfen, wurde ein t-Test bei unabhängiger Stichprobe durchgeführt. Daraus ergibt sich, dass kein signifikanter Unterschied zwischen den Gruppen vorliegt ($t(334) = .017$, $p = .986$). Der Nudge wurde von ca. 64% der Experimentalgruppe in den Fragen gesehen. Zusammenfassend muss die Hypothese H1 abgelehnt werden, denn unter Berücksichtigung aller demografischen Merkmale wie Alter, Geschlecht und Bildung ist der Unterschied zwischen der Experimental- und der Kontrollgruppe bezüglich der Selbstoffenbarung nicht signifikant ($t(334) = .017$, $p = .986$).

8.3 Einfluss des Risikobewusstseins (Hypothese H2a & H2b)

H2a: Das Risikobewusstsein hat keinen Effekt auf die Wirkung des Social-Norm-Digital-Nudges auf die Selbstoffenbarung.

H2b: Das Risikobewusstsein hat keinen Effekt auf die Selbstoffenbarung.

Anhand der Hypothesen 2a und 2b sollte herausgefunden werden, welchen Einfluss das Risikobewusstsein einer Person auf ihre Selbstoffenbarung und die Wirkung des Nudges auf sie aufweist. Mit einem Cronbach's Alpha Wert von 0.832 bei der Umfrage und 0.800 beim Pretest erreicht die Skala des Risikobewusstseins eine gute interne Konsistenz. Um dieser Frage nachzugehen, wurde eine lineare Regression berechnet. Das Resultat der Regression zeigt, dass das Risikobewusstsein einen signifikanten negativen Einfluss auf die Selbstoffenbarung ausübt ($F(11) = 4.689, p = .000$). Mit jedem Punkt auf der Skala des Risikobewusstseins sinkt die Selbstoffenbarung um 0.317 Punkte. Auf die Wirkung des Nudges hat das Risikobewusstsein hingegen keine Auswirkungen ($F(11) = 4.689, p = .611$).

Regression	Regressionskoeffizient B	t-Wert	Sig.
Gesamte Stichprobe (n = 312)			
Risikobewusstsein	-.317	-5.137	.000
Nudge X Risikobewusstsein	.031	.510	.756

Tabelle 7: Resultat der Regression für die Hypothesen H2a & H2b
Quelle: eigene Darstellung.

Das Risikobewusstsein wurde auf einer fünfstufigen Likert-Skala mit acht Items erfasst. Sein Wert kann von eins bis 40 variieren. Wenn Personen einzelne Angaben nicht getroffen haben, kann es vorkommen, dass der Wert unter acht sinkt, allerdings kann er null nicht erreichen.

Ein gewisses Risikobewusstsein konnte bei den meisten festgestellt werden. Das zeigt auch, dass nur 1.8% der gesamten Stichprobe angaben, ihre Privatsphäre sei in sozialen Netzwerken sicher. Die Hypothese H2a kann bestätigt werden, denn das Risikobewusstsein übt keinen signifikanten Einfluss auf die Wirkung des Social-Norm-Digital-Nudges aus ($F(11) = 4.689, p = .611$). Die Hypothese H2b muss allerdings abgelehnt werden, da das Risikobewusstsein einen signifikanten negativen Effekt auf die Selbstoffenbarung zeigt ($F(11) = 4.689, p = .000$). Personen mit einem hohen Risikobewusstsein teilen weniger Informationen als Menschen mit einem tiefen Wert für dieses.

8.4 Einfluss des Bedürfnisses nach Popularität (Hypothese H3a & H3b)

H3a: Das Bedürfnis nach Popularität schwächt die Wirkung des Social-Norm-Digital-Nudges auf die Selbstoffenbarung.

H3b: Das Bedürfnis nach Popularität hat einen positiven Effekt auf die Selbstoffenbarung.

Die Hypothesen H3a und H3b beziehen sich auf den Einfluss des Bedürfnisses nach Popularität. Der Cronbachs Alpha der Skala für das Bedürfnis von Popularität betrug beim Pretest 0.828 und bei der eigentlichen Umfrage 0.808, somit besteht eine gute interne Konsistenz. Das Resultat zeigt, dass zwar eine Wirkung des Bedürfnisses nach Popularität auf die Selbstoffenbarung vorhanden ist, diese aber nicht signifikant ist ($F(11) = 4.689, p = .064$). Hingegen konnte kein Effekt auf die Wirkung des Social-Norm-Digital-Nudges nachgewiesen werden ($F(11) = 4.689, p = .538$).

Regression	Regressionskoeffizient B	t-Wert	Sig.
Gesamte Stichprobe (n = 312)			
Bedürfnis nach Popularität	.128	1.862	.064
Nudge X Bedürfnis nach Popularität	-.042	-.616	.538

Tabelle 8: Resultat der Regression für die Hypothesen H3a & H3b.
Quelle: eigene Darstellung.

Allgemein zu bemerken sind die auffällig tiefen Werte: Auf einer Skala von eins bis 60 liegt der Maximalwert bei nur 43% und 50% der Werte der gesamten Stichprobe fallen zwischen 14 und 23. Abschliessend kann die Hypothese H2a abgelehnt werden, da das Bedürfnis nach Popularität keinen Einfluss auf die Wirkung des Nudges zeigt ($F(11) = 4.689, p = .538$). Die Hypothese H2b wird abgelehnt, da zwar grundsätzlich kein signifikanter Zusammenhang zwischen der Selbstoffenbarung und dem Bedürfnis nach Popularität besteht ($F(11) = 4.689, p = .064$).

8.5 Einfluss der Gruppenkonformität (Hypothese H4a & H4b)

H4a: Die Gruppenkonformität verstärkt die Wirkung des Social-Norm-Digital-Nudges auf das Selbstoffenbarungsverhalten.

H4b: Die Gruppenkonformität hat einen positiven Effekt auf das Selbstoffenbarungsverhalten.

Regression	Regressionskoeffizient B	t-Wert	Sig.
Gesamte Stichprobe (n = 312)			
Gruppenkonformität	.070	.748	.455
Nudge X Gruppenkonformität	.016	.178	.858

Tabelle 9: Resultat der Regression für die Hypothesen H4a & H4b.
Quelle: eigene Darstellung.

Der Cronbachs Alpha der Skala für Gruppenkonformität betrug im Pretest 0.786 und im der Umfrage 0.843, was einer akzeptablen internen Konsistenz beim Pretest und einer guten internen Konsistenz bei der Umfrage entspricht. Die lineare Regression hat ergeben, die Gruppenkonformität weder auf die Wirkung des Social-Norm-Digital- noch auf die Selbstoffenbarung einen signifikanten Einfluss ausübt. Die Werte für die Gruppenkonformität fallen tendenziell niedrig aus. Die Hypothese H4a kann aufgrund des Resultates der Regression abgelehnt werden ($F(11) = 4.689$, $p = .858$). Ebenso wird die Hypothese H4b revidiert ($F(11) = 4.689$, $p = .455$).

8.6 Berücksichtigung der demografischen Merkmale

Bei der Auswertung der Daten ist aufgefallen, dass sich die Selbstoffenbarung in den Altersgruppen deutlich unterscheidet. So liegt beispielsweise der Mittelwert der Selbstoffenbarung bei den 19- bis 24-Jährigen bei zehn und bei den 25- bis 35-Jährigen bei sieben. Daher erscheint die Vermutung naheliegend, dass das Alter einen grösseren Effekt haben könnte auf die Wirkung des Nudges, da die 19- bis 24-Jährigen 50% der Stichprobe ausmachen. Um dieser Vermutung auf den Grund zu gehen, wurden die Auswertungen erneut vorgenommen, allerdings ohne Berücksichtigung der 19- bis 24-Jährigen und derjenigen, die keine Angaben zum Alter getroffen hatten. Dadurch reduzierte sich die Grösse der Stichprobe auf 155 Teilnehmende. Zudem lag das Durchschnittsalter neu bei 34.35 Jahren. Die Auswertungen zeigten deutliche Unterschiede: Beispielsweise wurde die mit dem Nudge unterstützte Option in der Experimentalgruppe 12.9% häufiger ausgewählt als in der Kontrollgruppe. Wenn die Altersgruppe 19–24 inkludiert wird, gilt dies für 0% der Befragten. Durch die Faktoren Alter, Rauchen, Alkohol, besuchte Orte, E-Mail und Telefonnummer wird die Wirkung des Nudges verstärkt, wenn die Altersgruppe 19–24 miteinbezogen wird. Ansonsten wird die Wirkung verschlechtert. Insgesamt wurde die Option des Nudges von der Experimentalgruppe 26.9% häufiger ausgewählt als in der Kontrollgruppe, was auf eine starke Wirkung des Social-Norm-Digital-Nudges hinweist. Ebenfalls wurde von der Experimentalgruppe 22.9% häufiger eine kleinere Zielgruppe selektiert.

8.6.1 Wirkung des Nudges auf die Selbstoffenbarung (Hypothese 1)

Mit dem veränderten Datensatz wurde die Hypothese erneut geprüft. Der Mittelwert der Experimentalgruppe ($M = 7.12$, $SD = 6.007$, $n = 74$) unterscheidet sich deutlicher von dem der Kontrollgruppe ($M = 9.15$, $SD = 7.201$, $n = 171$) als zuvor. Durch das Entfernen der Altersgruppe 19–24 konnte kein signifikanter Unterschied in der Selbstoffenbarung

festgestellt werden ($t(153) = -1.842, p = .067$). Im Vergleich der Experimentalgruppe und der Kontrollgruppe mit und ohne die Altersgruppe 19–24 kann festgestellt werden, dass sich hauptsächlich die Experimentalgruppen unterscheiden, denn der Mittelwert ist hier deutlich niedriger (mit: $M = 9.13$, ohne: $M = 7.12$). Hingegen veränderte sich in der Kontrollgruppe kaum ein Parameter. Der Mittelwert erhöhte sich beispielsweise leicht (mit: $M = 9.12$, ohne: $M = 9.15$).

Attribute (Option vom Nudge)	Restriktiver als der Nudge [%]	Option des Nudges [%]	Offener als der Nudge [%]
Alter (Freunde)	+7.5	-3.0	-4.5
Probanden mit Nudge	58.1	36.5	5.4
Probanden ohne Nudge	50.6	39.5	9.9
Beziehungsstatus (enge Freunde)	-0.2	12.9	-12.7
Probanden mit Nudge	55.4	20.3	24.3
Probanden ohne Nudge	55.6	7.4	37.0
Sexuelle Orientierung (enge Freunde)	+12.6	+3.2	-15.8
Probanden mit Nudge	74.3	8.1	17.6
Probanden ohne Nudge	61.7	4.9	33.4
Religion (nur ich)		+10.3	-10.3
Probanden mit Nudge		75.7	24.3
Probanden ohne Nudge		65.4	34.6
Partei (enge Freunde)	-10.4	+8.6	+1.8
Probanden mit Nudge	64.9	13.5	21.6
Probanden ohne Nudge	75.3	4.9	19.8
Rauchen (Freunde)	-3.3	+1.0	-2.3
Probanden mit Nudge	73.1	12.1	14.8
Probanden ohne Nudge	76.4	11.1	12.5
Alkohol (Freunde)	+9.8	-3.8	-6.0
Probanden mit Nudge	85.1	13.5	1.4
Probanden ohne Nudge	75.3	17.3	7.4
Krankheiten (nur ich)		-0.7	+0.7
Probanden mit Nudge		91.9	8.1
Probanden ohne Nudge		92.6	7.4

Heimadresse (nur ich)		+0.7	-0.7
Probanden mit Nudge		79.7	20.3
Probanden ohne Nudge		79.0	21.0
Besuchte Orte (Freunde)	+6.7	-6.0	-0.7
Probanden mit Nudge	48.6	44.6	6.8
Probanden ohne Nudge	42.0	50.6	7.4
E-Mail-Adresse (nur ich)		+3.2	-3.2
Probanden mit Nudge		64.9	35.1
Probanden ohne Nudge		61.7	38.3
Telefonnummer (nur ich)		+0.5	-0.5
Probanden mit Nudge		77.0	23.0
Probanden ohne Nudge		76.5	23.5
Summe der Differenzen	+22.7	+26.9	-49.6

Tabelle 10: Unterschiede in der Wahl der Teilen Option zwischen Experimental- und Kontrollgruppe (ohne Alter 19–24).

Quelle: eigene Darstellung. Bemerkung: Die Experimentalgruppe wird hier mit der Kontrollgruppe verglichen. Dabei stellt ein positiver Wert eine häufigere Auswahl der Option bei der Experimentalgruppe dar und ein negativer Wert eine häufigere Selektion in der Kontrollgruppe.

Die gleiche Untersuchung wurde auch für das Geschlecht vorgenommen. Bei der Untersuchung des Mittelwertes konnte festgestellt werden, dass sich dieser nur zwischen dem Geschlecht unterscheidet und nicht zwischen den Gruppen. Der Mittelwert der weiblichen Teilnehmerinnen (Experimentalgruppe: $M = 7.73$, Kontrollgruppe: $M = 7.24$) war zwar deutlich niedriger als der bei den Männern (Experimentalgruppe: $M = 9.76$, Kontrollgruppe: $M = 11.04$), aber der Unterschied zwischen der Experimental- und der Kontrollgruppen ist weder bei Männern ($t(166) = -1.063$, $p = .290$) noch bei Frauen ($t(151) = 0,509$, $p = .611$) signifikant. Die Teilnehmenden, die bei der Frage nach dem Geschlecht die Option <divers> nutzten, wurden alle der Kontrollgruppe zugewiesen. Daher konnte nicht überprüft werden, welchen Einfluss der Nudge auf Personen mit dieser Identifikation aufweist. Schlussendlich kann erkannt werden, dass Männer eine signifikant höhere Selbstoffenbarung zeigen als Frauen ($t(319) = -3.678$, $p = .000$). Zudem scheint bei Männern der Nudge eine etwas stärkere Wirkung gehabt zu haben.

Beim Bildungsniveau wurden die Mittelwerte ebenfalls verglichen. Es konnte festgestellt werden, dass Bachelor- und Master-Absolventinnen sowie -Absolventen und Inhaber/-innen eines Eidgenössischen Diploms oder Fachausweises niedrigere Mittelwerte er-

reichten als Befragte mit anderen Bildungsabschlüssen. Der Social-Norm-Digital-Nudge scheint Personen mit der Berufslehre als höchsten Abschluss sogar zu animieren, mehr zu teilen. Mit dieser Ausnahme konnte bei keinem Bildungsniveau ein signifikanter Unterschied festgestellt werden.

Bildungsniveau	Mittelwert		t-Wert	Sig.
	Experimentalgruppe	Kontrollgruppe		
obligatorische Schule	8.2	10.67	-*	-*
Berufslehre	11.97	8.54	1.887	.064
Berufsmaturität	9.13	10.27	-.644	.552
gymnasiale Maturität oder Fachmaturität	9.33	9.35	-.007	.995
Bachelor FH, Uni oder ETH	6.83	8.16	-.990	.325
Master FH, Uni oder ETH	6.77	9.38	-*	-*
Eidg. Diplom/Fachausweis	7.00	7.75	-*	-*
Diplom höhere Fachschule	10.80	15.73	-*	-*

Tabelle 11: Mittelwerte der Selbstoffenbarung im Vergleich zum Bildungsniveau.

Quelle: eigene Darstellung. Bemerkung: * bedeutet, dass das Vornehmen eines t-Tests aufgrund der zu kleinen Stichprobe nicht möglich war.

Ebenfalls wurde die Erwerbstätigkeit betrachtet. Die Mittelwerte fallen ähnlich aus, ausser bei denen, die für eine geringe Anzahl von Personen gelten (Mutterschaftsurlaub, Erwerbstätigkeit im Studium und in Ausbildung/Umbildung). Bei den Pensionierten und den nicht Erwerbstätigen scheint der Social-Norm-Nudge gegenteilig zu wirken, denn der Mittelwert der Selbstoffenbarung ist bei denen höher, die den Nudge erhalten haben, als bei denen, die ihn nicht erhalten haben.

Erwerbstätigkeit	Mittelwert		t-Wert	Sig.
	Experimentalgruppe	Kontrollgruppe		
erwerbstätig (Vollzeit)	9.32	9.84	-.371	.711
erwerbstätig (Teilzeit)	8.15	8.40	-.202	.840
erwerbstätig (Studium)	11.00	21.00	.*	.*
Mutterschafts-/Erziehungsurlaub oder Beurlaubung	2.00	k/A	.*	.*
in Ausbildung/Umbildung	10.33	9.71	.*	.*
nicht erwerbstätig/pensioniert	9.32	8.07	.683	.498

Tabelle 12: Mittelwerte der Selbstoffenbarung im Vergleich zur Erwerbstätigkeit.

Quelle: eigene Darstellung. Bemerkung: * bedeutet, dass das Vornehmen eines t-Tests aufgrund der zu kleinen Stichprobe nicht möglich war.

Zuletzt wurde auch überprüft, ob Erfahrungen mit Risiken die Wirkung des Nudges auf das Selbstoffenbarungsverhalten beeinflussen könnte. Mit Cyberstalking hatten 9.7% der Stichprobe bereits Erfahrung gesammelt. Der Nudge hat bei Personen mit diesem Hintergrund zu einer Erhöhung des Mittelwertes geführt. Hingegen bei Personen, die keine Erfahrung mit Cyberstalking mitbrachten, verringerte sich der Mittelwert, sofern ein Nudge eingesetzt wurde. Das gleiche Verhalten gilt für das Risiko, dass persönliche Informationen ohne Kenntnis der betroffenen Person veröffentlicht werden (18.7% der Person aus der Stichprobe). Nur bei Vorliegen eines Identitätsdiebstahls auf sozialen Netzwerken, zu dem 5.2% der Stichprobe angaben, bereits Erfahrungen zu haben, konnte der Nudge das Selbstoffenbarungsverhalten verringern. Die Erfahrung senkt zwar die Selbstoffenbarung in den meisten Fällen, beim Hinzufügen eines Nudges wird der Wert allerdings teilweise sogar von ihr erhöht. Daher kann schlussfolgert werden, dass die Wirkung des Nudges eher negativ beeinflusst wird.

Risiko	Erfahrung	Mittelwert	
		Experimentalgruppe	Kontrollgruppe
Cyberstalking	Ja	9.93	8.13
	Nein	8.85	9.25
Veröffentlichung von persönlichen Daten ohne Kenntnis	Ja	8.26	8.10
	Nein	8.95	9.42
Identitätsdiebstahl in sozialen Netzwerken	Ja	8.67	10.82
	Nein	9.12	9.04

Tabelle 13: Selbstoffenbarung im Vergleich zur Erfahrung mit Risiken.
Quelle: eigene Darstellung.

Unter genauerer Betrachtung kann festgestellt werden, dass beim Entfernen der Altersgruppe 19–24 und derjenigen Personen, die keine Angaben zu ihrem Alter getroffen hatten, der Unterschied zwischen den Gruppen erhöht wird, allerdings trotzdem keinen signifikanten Wert annimmt, wenn auch dieser nur knapp verfehlt wurde ($t(153) = -1.842$, $p = .067$). Es ist auch zu beachten, dass durch das Entfernen dieser Altersgruppe knapp 53% der gesamten Stichprobe unbeachtet bleiben. Allerdings ist es unklar, wie das Ergebnis bei einer proportionalen Altersverteilung ausfallen würde.

8.6.2 Einfluss des Risikobewusstseins (Hypothese H2a & H2b)

Zur Überprüfung dessen, ob die überproportionale Vertretung der Altersgruppe 19–24 einen Effekt auf das Resultat hat, wurde die Regression bei der Hypothese 2a und 2b ebenfalls ohne diese berechnet. Das Ergebnis hat sich nur leicht verändert, ohne dass die Signifikanz modifiziert wurde (Risikobewusstsein: $F(11) = 3.174$, $p = .005$; Nudge X Risikobewusstsein: $F(11) = 3.174$, $p = .221$). Folglich ist das Resultat unabhängig von der Altersgruppe.

Regression	Regressionskoeffizient B	t-Wert	Sig.
Gesamte Stichprobe (n = 312)			
Risikobewusstsein	-.317	-5.137	.000
Nudge X Risikobewusstsein	.031	.510	.756
Stichprobe ohne die Altersgruppe 19–24 (n = 149)			
Risikobewusstsein	-.247	-2.859	.005
Nudge X Risikobewusstsein	.104	1.231	.221

Tabelle 14: Resultat der Regression für die Hypothesen H2a & H2b unter Berücksichtigung des Alters.
Quelle: eigene Darstellung.

Die Werte des Risikobewusstseins unterscheiden sich nach Alter, Geschlecht, Bildungsniveau und Erwerbstätigkeit kaum voneinander: Bei den Altersgruppen haben bis 18-Jährige und 19- bis 24-Jährige den niedrigsten Mittelwert ($M = 22$) und die Altersgruppe 35–44 den höchsten Mittelwert ($M = 26$). Männliche Probanden erreichten einen Mittelwert von 22, weibliche von 24 und Personen mit der Angabe «divers» von 23. Frauen verfügen im Durchschnitt über ein höheres Risikobewusstsein, was ihre signifikant niedrigere Selbstoffenbarung erklärt. Beim Bildungsniveau fällt das Resultat ähnlich aus – hier zeigen Personen mit der Berufslehre und dem Diplom höhere Fachschule als höchsten Abschluss den niedrigsten Mittelwert ($M = 22$). Personen mit einem Master oder einem Eidgenössischen Diplom erreichten den höchsten Mittelwert ($M = 26$). Bei der Erwerbstätigkeit gibt es einzelne Ausreißer, die den Mittelwert nach unten bzw. nach oben ziehen. Den niedrigsten Mittelwert ($M = 16$) weisen diejenigen auf, die neben dem Studium einer Erwerbstätigkeit nachgehen, und den höchsten Mittelwert ($M = 33$) weist die Person auf, die sich im Mutterschaftsurlaub oder einer sonstigen Beurlaubung befindet, gefolgt von Personen, die einer Teilzeit Erwerbstätigkeit nachgehen ($M = 24$). Von diesen Fällen abgesehen liegen die Mittelwerte bei der Unterteilung nach Erwerbstätigkeit ebenfalls zwischen 21 und 24. Über die gesamte Stichprobe hinweg befanden sich 50% der Werte zwischen 18 und 27.

Zusammenfassend kann gefolgert werden, dass alle Befragten ein ähnliches Risikobewusstsein aufweisen, unabhängig von ihren demografischen Angaben.

8.6.3 Einfluss des Bedürfnisses nach Popularität (Hypothese H3a & H3b)

Auch bei dieser Hypothese wurde der Einfluss der Altersgruppe 19–24 genauer untersucht. Es zeigt sich, dass durch ihr Entfernen aus der Auswertung das Bedürfnis nach Popularität seinen Einfluss sowohl auf die Selbstoffenbarung als auch auf die Wirkung

des Nudges verliert. Diese deutet darauf hin, dass der Effekt in der Altersgruppe 19–24 stärker vorhanden ist. Daher wurde ebenfalls untersucht, ob bei der Altersgruppe 19–24 ein signifikanter Einfluss des Bedürfnisses nach Popularität besteht. Tatsächlich konnte beim Durchführen der Regression für diese Gruppe ein signifikanter positiver Einfluss des Bedürfnisses nach Popularität auf die Selbstoffenbarung festgestellt werden ($F(11) = 3.407, p = .005$).

Regression	Regressionskoeffizient B	t-Wert	Sig.
Gesamte Stichprobe (n = 312)			
Bedürfnis nach Popularität	.128	1.862	.064
Nudge X Bedürfnis nach Popularität	-.042	-.616	.538
Stichprobe ohne Altersgruppe 19–24 (n = 149)			
Bedürfnis nach Popularität	-.016	-.156	.876
Nudge X Bedürfnis nach Popularität	-.010	-.092	.927
Stichprobe nur Altersgruppe 19–24 (n = 163)			
Bedürfnis nach Popularität	.260	2.818	.005
Nudge X Bedürfnis nach Popularität	-.099	-1.091	.277

Tabelle 15: Resultat der Regression für die Hypothesen H3a & H3b unter Berücksichtigung des Alters.
Quelle: eigene Darstellung.

Das Bedürfnisses nach Popularität nimmt grundsätzlich ab, je älter Personen werden. Das zeigt sich auch anhand der Mittelwerte (< = 18: $M = 20$, 35–44: $M = 19$, 65+: $M = 17$). Personen, die beim Geschlecht die Option «divers» nutzten, erreichten im Durchschnitt den höchsten Mittelwert, gefolgt von Frauen (divers: $M = 23$, weiblich: $M = 20$, männlich: $M = 19$). Nach dem Bildungsniveau differenziert haben vor allem Personen, die eine gymnasiale Maturität oder eine Fachmaturität als höchsten Abschluss besitzen, ein hohes Bedürfnis nach Popularität ($M = 22$). Am niedrigsten ist der Mittelwert bei Personen, die einen Masterabschluss aufweisen ($M = 15$). Bei der Erwerbstätigkeit zeigt sich, dass Personen mit einer Vollzeittätigkeit den niedrigsten Mittelwert zeigen ($M = 18$) und Befragte, die entweder im Mutterschaftsurlaub sind oder einer sonstigen Beurlaubung unterliegen, den höchsten Mittelwert erreichen ($M = 26$) – gefolgt von Personen, die neben dem Studium einer Erwerbstätigkeit nachgehen ($M = 21$).

Die Hypothese H2a kann auch unter Berücksichtigung des Alters ebenfalls abgelehnt werden. Hingegen wird die Hypothese H2b nur teilweise abgelehnt, da zwar grundsätzlich kein signifikanter Zusammenhang zwischen der Selbstoffenbarung und dem Bedürf-

nis nach Popularität besteht ($F(11) = 4.689$, $p = .064$), er in der der Altersgruppe der 19- bis 24-Jährigen aber zu beobachten ist ($F(11) = 3.407$, $p = .005$).

8.6.4 Einfluss der Gruppenkonformität (Hypothese H4a & H4b)

Durch das Entfernen der genannten Altersgruppe konnte der Einfluss auf die Selbstoffenbarung leicht verändert werden, was darauf hindeutet, dass die Gruppenkonformität bei älteren Personen die Selbstoffenbarung eher beeinflusst. In der Wirkung des Nudges scheint das Alter hingegen keinen Unterschied zu machen.

Regression	Regressionskoeffizient <i>B</i>	<i>t</i> -Wert	Sig.
Gesamte Stichprobe (n = 312)			
Gruppenkonformität	.070	.748	.455
Nudge X Gruppenkonformität	.016	.178	.858
Stichprobe ohne Altersgruppe 19–24 (n = 149)			
Gruppenkonformität	.191	1.450	.149
Nudge X Gruppenkonformität	-.024	-.188	.851

Tabelle 16: Resultat der Regression für die Hypothesen H4a & H4b unter Berücksichtigung des Alters.
Quelle: eigene Darstellung.

Frauen und Personen mit dem Geschlecht <divers> haben eine leicht höhere Gruppenkonformität als Männer (weiblich & divers: $M = 15$, männlich: $M = 14$). Personen mit einem Masterabschluss oder einem Eidg. Diplom zeigten den niedrigsten Mittelwert ($M = 11$) und Personen mit gymnasialer Maturität oder Fachmaturität den höchsten ($M = 16$). Nach der Erwerbstätigkeit unterschieden erreichten Befragte mit einer Vollzeitberufstätigkeit oder Studenten mit einem Job den niedrigsten Mittelwert ($M = 13$) und Personen in Ausbildung oder in Mutterschaftsurlaub oder Beurlaubung den Höchsten ($M = 16$). Die demografischen Merkmale scheinen bei der Gruppenkonformität eine geringe Rolle zu spielen.

8.7 Fazit der Resultate

Im Rahmen der Auswertung der Hypothesen konnte festgestellt werden, dass unter Berücksichtigung der Altersgruppe gewisse Annahmen als korrekt befunden werden könnten. Nichtsdestotrotz konnte der Social-Norm-Digital-Nudge, wenn die gesamte Stichprobe betrachtet wird, keine niedrigere Selbstoffenbarung verursachen. Nachdem die Altersgruppe 19–24 entfernt wurde, wurde ein signifikantes Ergebnis nur knapp verfehlt. Ebenso haben die intervenierenden Variablen keinen Einfluss auf die Selbstoffenbarung

bzw. die Wirkung des Social-Norm-Digital-Nudges. Nur das Risikobewusstsein bestimmt die Selbstoffenbarung.

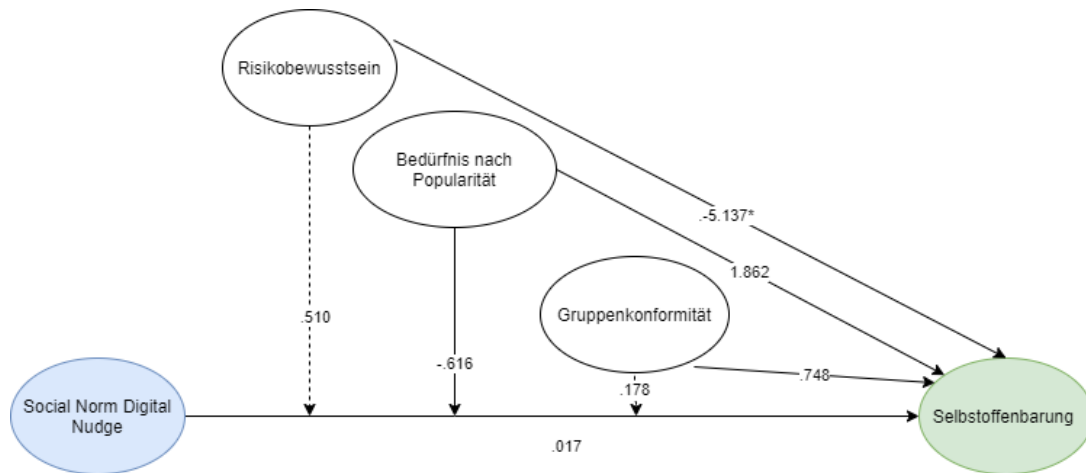


Abbildung 5: Hypothesenmodell (nach der Auswertung).

Quelle: eigene Darstellung. Bemerkung: * $p = .000$

9 Diskussion

Im folgenden Kapitel wird der Forschungsstand, der in den ersten Kapiteln aufgearbeitet wurde, verglichen mit den Erkenntnissen der Untersuchungen. Die vorliegende Untersuchung, die im Rahmen einer Bachelorarbeit durchgeführt wurde, wird in diesem Kapitel kritisch reflektiert. Dabei wird auf Punkte eingegangen, die in einer möglichen anknüpfenden Studie verbessert werden sollten. Dabei soll vor allem die Ausführung des Experiments beachtet werden.

9.1 Ergebnisdiskussion

Anhand der Ergebnisse dieser Bachelorarbeit lässt es sich nicht wissenschaftlich belegen, dass Personen bei Verwendung eines Social-Norm-Digital-Nudges weniger Inhalte in sozialen Netzwerken teilen bzw. diese bewusster selektieren. Doch die erhobenen Daten zeigen, dass die Resultate nicht zu verallgemeinern sind: So konnte festgestellt werden, dass der Social-Norm-Digital-Nudge bei einigen Selbstoffenbarungsattributen stärker wirkte als bei anderen. Beispielsweise funktioniert der Nudge beim Attribut Rauchen deutlich besser als beim Attribut «sexuelle Orientierung». Auch mit dem Entfernen der Altersgruppe der 19- bis 24-Jährigen verändern sich die Selbstoffenbarungsattribute deutlich. Die Privatsphäre ist stark kontextabhängig (Morando et al., 2014, S. 6–7). Zudem definiert jede Person Attribute, die ihre Privatsphäre kennzeichnen, unterschiedlich (Kokolakis, 2017, S. 127). Das zeigt, dass die Definition von Altman (1981, S. 18) ihre Gültigkeit behält und die Privatsphäre einer selektiven Kontrolle unterliegt, die für jede Person anders interpretiert wird. So haben vermutlich einige Personen gewisse Informationen als intimer ausgelegt als andere. Tendenziell sind die Mittelwerte in der Experimental- wie auch in der Kontrollgruppe niedrig: Auf einer Skala von null bis 36 liegt der Durchschnitt bei beiden Gruppen bei neun. Daher kann vermutet werden, dass viele Personen viele Attribute als intim annehmen. In einer Untersuchung von Masur und Scharkow (2016) wird untermauert, dass Informationen nicht oder weniger häufig geteilt werden, wenn sie von der sie besitzenden Person als privat eingestuft werden. Unklar bleibt es, warum der Nudge bei 19- bis 24-Jährigen weniger gut zu funktionieren scheint als bei Älteren. Zum einen liegt dies vermutlich daran, dass diese Altersgruppe zu 36.9% keinen Facebook-Account nutzt und nur 8.3% von ihr die Plattform mehrmals täglich verwenden. Zum Vergleich verwenden die 25- bis 34-jährigen Facebook zu 21.5% täglich und nur 19% von ihnen verfügen über keinen Facebook-Account. Die Optionen wurden von Facebook übernommen und das Szenario inklusive der Bilder stammte auch von hier. Dadurch könnten viele Personen in der

Altersgruppe nicht mit ihnen vertraut gewesen sein. Neue soziale Netzwerke sind teilweise mit weniger Optionen ausgestattet, um die soziale Privatsphäre zu schützen. Zudem ist die Konstruktionsweise neuer sozialer Netzwerk in Bezug auf das Teilen von Informationen stark unterschiedlich (Bernath et al., 2020, S. 62–63). Die Umgebung scheint einen starken Einfluss auszuüben (Kokolakis, 2017, S. 12), so waren viele Personen in dieser Gruppe vermutlich nicht vertraut mit dem Aussehen von Facebook. Vermutlich konnten die Befragten dieser Altersgruppe auch keine Assoziationen zur Social-Norm-Aussagen «Die meisten Personen auf Facebook» bilden. Doch folgt daraus nicht, dass sich Jüngere generell weniger um ihre Privatsphäre kümmern: Wenn auch der Nudge bei ihnen weniger stark zu einer Verringerung der geteilten Informationen beigetragen hat als bei Älteren, ist die Selbstoffenbarung im Durchschnitt eher tief. Zudem haben auch ältere Altersgruppen einen gesteigerten Selbstoffenbarungswert gezeigt. Auch andere Untersuchungen zeigen, dass vor allem jüngere Personen dazu neigen, ihre Einstellungen anzupassen und sich um ihre Privatsphäre zu sorgen (Bernath et al., 2020; Blank et al., 2014; Boyd & Hargittai, 2010). Ein möglicher Einflussfaktor könnte darin bestehen, dass Personen aus der Altersgruppe 19–24 bewusster entscheiden, mit wem sie welche Inhalte teilen wollen, und durch den Nudge vorgeschlagene Option deshalb ignorierten. Der Nudge zeigt schlussendlich nicht immer die tiefste Option an, hätte jedoch jede/r Befragte exakt nach ihm gewählt, wäre ein Wert von elf entstanden.

Unterschiede zeichnen sich auch beim Geschlecht ab, so zeigen Männer eine signifikant höhere Selbstoffenbarung als Frauen. Ebenso reagieren Männer stärker als Frauen auf den Nudge. Bei ersteren konnte der Mittelwert um, wenn auch nicht signifikante, 1.28 Punkte gesenkt werden und bei Frauen wurde er mithilfe des Nudges um 0.49 Punkte erhöht. Bei Frauen ist der Wert grundsätzlich tief, dafür ist bei ihnen das Risikobewusstsein stärker ausgeprägt als bei Männern. Ebenso haben mehr Frauen als Männer Erfahrungen mit Risiken gehabt. Diese Resultate decken sich mit den Erkenntnissen der JAMES-Studie (2020), in der bei Mädchen ebenfalls ein höheres Risiko sowie mehr zum Schutz der Privatsphäre genutzte Einstellungen festgestellt wurden (Bernath et al., 2020, S. 50–51). Die Erfahrung mit Risiken der Selbstoffenbarung oder generell negative Erfahrungen in sozialen Netzwerken könnten eine mögliche Begründung der unterschiedlichen Werte der Selbstoffenbarung sowie des Risikobewusstseins sein.

Eine relevante Erkenntnis konnte auch zum Risikobewusstsein abgeleitet werden. Obwohl in Studien (Cheung et al., 2015; Taddicken, 2014) und im Privacy Paradox (Gerber et al., 2017, S. 142) ein fehlender Zusammenhang zwischen dem Risikobewusstsein und der Selbstoffenbarung gesehen wird, konnte in dieser Untersuchung einer festgestellt

werden. Aussagen hierzu beruhen auf hypothetischen Einstellungen der Umfrageteilnehmer/-innen. Nichtsdestotrotz ist eine starke Signifikanz festzustellen. Das kann daran liegen, dass die an dieser Untersuchung teilnehmenden Personen zuvor stärker zu ihrer sozialen Privatsphäre befragt worden waren und weniger häufig zur institutionellen Privatsphäre. Untersuchungen zeigen auch, dass sich Menschen um die soziale Privatsphäre mehr Sorgen machen als um die institutionelle (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). Zusätzlich wurden auf der Risikobewusstseinsskala dieser Arbeit bewusst Items gewählt, anhand deren sich die soziale Privatsphäre messen lässt. Die Differenzierung zwischen sozialer und institutioneller Privatsphäre könnte eine mögliche Erklärung für die Unterschiede zu den Untersuchungen von Taddicken (2014) und Cheung et al. (2015) bilden.

Der Einflussfaktor «Bedürfnis nach Popularität» war knapp nicht signifikant. Allerdings konnte in der Altersgruppe der 19- bis 34-Jährigen festgestellt werden, dass der Faktor einen signifikanten Einfluss auf die Selbstoffenbarung nimmt. Die Vermutung liegt daher nahe, dass die Konstruktionsweise neuer sozialer Netzwerke, die von dieser Altersgruppe hauptsächlich genutzt wird, einen möglichen Grund für dieses unterschiedliche Verhalten darstellt, denn sie belohnt vor allem diejenigen Personen, die viele Inhalte teilen, mit einer hohen Reichweite, die notwendig ist, um viele Personen zu erreichen (Bernath et al., 2020, S. 62–63).

Zusammenfassend ist zu erkennen, dass ein Social-Norm-Digital-Nudge in einigen Fällen nicht wirkungslos ist, sein Effekt aber stark kontextabhängig ist. Einigen Personen konnte der Nudge helfen, gewisse Informationen mit einer kleineren Zielgruppe zu teilen. Es stellt sich die Frage, ob Konzerne wie Facebook solche Nudges verwenden möchten. Da zu einem soziale Netzwerke ihr Geschäftsmodell auf Inhalten der Nutzenden aufbauen, welche für die Umsatzgenerierung wesentlich ist (Abramova et al., 2017, S. 1). Figi und Lehrer (2020, S. 8) vermuten allerdings, dass durch die Anwendung von Nudging zum Schutz der sozialen Privatsphäre auch das Vertrauen in das Unternehmen und das Netzwerk gesteigert werden kann, was zur Erhöhung der Interaktion führen könnte. Zudem bestehen vermutlich nicht alle viralen Inhalte aus persönlichen Details. Neben den Nudges wäre auch eine Vereinheitlichung der Einstellungen zum Schutz der Privatsphäre sinnvoll, da einige Netzwerke ihre User/innen auf granularen Ebenen die Privatsphäre regulieren lassen und andere (nur auf Profilebene) wenige Optionen für Endanwenderinnen und -anwender bieten.

9.2 Grenzen der Arbeit

Die Stichprobenerfassung erwies sich als effektiv, da über 350 Teilnehmende gefunden werden konnten und nur etwa 11% von ihnen aufgrund inkorrekten/unseriösen Ausfüllens der Umfrage aus der Stichprobe entfernt werden mussten. Aufgrund der Beschränkung auf das soziale Umfeld des Verfassers in der Suche nach Befragten sind gewisse Altersklassen in der Stichprobe überproportional stark vertreten. Bei einer erneuten Umfrage müssten Methoden evaluiert werden, um auch vermehrt andere Altersklassen zur Teilnahme zu motivieren. Beispielsweise könnten Strassenbefragungen durchgeführt werden oder die Umfrage könnte gezielt in verschiedenen Unternehmungen verteilt werden. Eine andere Möglichkeit bietet die Begrenzung der Teilnahme auf eine gewisse Anzahl an Teilnehmenden einer Altersgruppe.

Neben der Stichprobenerfassung könnte auch das Erhebungsdesign angepasst werden. So könnte versucht werden, die effektiven Einstellungen auf Facebook oder einem anderen Netzwerk unter Beachtung des Datenschutzes zu sammeln, denn gemäss Kokolakis (2017, S. 127) sind Umfragen nicht geeignet, um das Verhalten einer Person effektiv zu messen. Der Fokus soll eher auf Einstellungsdaten liegen, d. h. auf Daten, die zeigen, wie Personen ihre Privatsphäre-Einstellungen gesetzt haben (Kokolakis, 2017, S. 132). Zwar wurde bereits eine Untersuchung dieser Art durchgeführt, in der die Vorstellung mit der tatsächlichen Einstellung verglichen und eine Diskrepanz festgestellt wurde (Liu et al., 2011, S. 1). Diese scheint allerdings auf der Kompetenz der Nutzenden zu basieren. Zudem stellt sich die Frage, ob eine entsprechende Untersuchung im Rahmen einer Bachelorarbeit möglich wäre und ob Personen bereit wären, dafür notwendige Daten zu teilen. Für die weitere Forschung wäre eine Untersuchung der Wirkung eines Social-Norm-Digital-Nudges in einem realen Sozialen Netzwerk vielversprechend.

Auch ist am Erhebungsdesign die Skala zur Erfassung des Bedürfnisses nach Popularität auszuwerten. Hier stellt sich die Frage, wie ehrlich die Teilnehmenden geantwortet haben, denn die erhaltenen Werte sind auffallend niedrig. Der Effekt durch die Reihenfolge der Items konnte aufgrund der zufälligen Anordnung der Items ausgeschlossen werden. Hier könnten bei einer erneuten Befragung bewusst gegensätzliche Items beziehungsweise Items mit dem Zweck, die Ehrlichkeit der Antworten zu messen, eingebaut werden. Wie bereits in der Ergebnisdiskussion erwähnt wurde, könnte die nachgeahmte Facebook Umgebung auch eine Rolle darin gespielt haben, dass vor allem Personen aus der Altersklasse 19–24 nicht auf die Nudges reagierten. Bei einer weiteren Untersuchung wäre es gegebenenfalls sinnvoll, die Teilnahme zu beschränken, beispielsweise auf Facebook-Nutzende. Dadurch könnte der Einfluss der Umgebung reduziert werden. Zusätzlich

müsste bei der nächsten Befragung die Kontrollfrage gegebenenfalls besser gekennzeichnet werden, um Verwirrung bei den Teilnehmenden vorzubeugen.

Zuletzt konnte festgestellt werden, dass der Social-Norm-Digital-Nudge teilweise höhere Selbstoffenbarung forcierte als die Mehrheit der Teilnehmenden. Daher wäre es sinnvoll, die Nudge-Option nicht zu variieren. Allerdings muss beachtet werden, dass die soziale Norm nicht zu unglaublich wird, denn dies könnte ihre Wirkung einschränken.

10 Fazit

In dieser Arbeit wurde folgende forschungsleitende Frage untersucht: Inwiefern können Social-Norm-Digital-Nudges das Verhalten von Personen dahingehend beeinflussen, dass sie weniger Daten bei der Verwendung von sozialen Netzwerken preisgeben? Nach der Aufarbeitung des Forschungsstands und Auswertung der empirischen Untersuchung kommt diese Arbeit zu folgendem Ergebnis.

Ein Social-Norm-Digital-Nudges kann kontext- und umgebungsabhängig Personen teilweise dazu bringen weniger Daten preiszugeben, sofern der Nudge eine niedrigere Selbstoffenbarung forciert. Zwar konnte in der vorliegenden Bachelorarbeit kein signifikanter Nachweis der Wirkung eines Social-Norm-Digital-Nudges erbracht werden, jedoch wurde die Wirkung eines Nudges identifiziert. Zudem wurden Erkenntnisse zu den Einflüssen auf diese gewonnen, vor allem zum Risikobewusstsein sowie zum Bedürfnis nach Popularität. Aufgrund der Tatsache, dass gewissen Kontextfaktoren wie der Umgebung des sozialen Netzwerks oder auch dem Alter zu wenig Beachtung geschenkt wurde, könnte auf Basis der vorliegenden Erkenntnisse in einer neuen Untersuchung ein signifikanter Nachweis dieses stark kontextabhängigen Themas angestrebt werden. Der Einsatz von Social-Norm-Digital-Nudges ist im Bereich der Privatsphäre allerdings im Allgemeinen sinnvoll. So konnten bei einigen Privatsphärenattributen im Vergleich zur Kontrollgruppe deutliche Veränderungen der Option herbeigeführt werden.

Es wird stetig wesentlicher, dass auch soziale Netzwerke den Schutz der Privatsphäre ihrer Nutzenden vorantreiben, denn sie können aufgrund der fehlenden Zahlungsbereitschaft keine Gebühren für die Nutzung erheben (Falch et al., 2009, S. 20–22). Das bedeutet im Umkehrschluss, dass soziale Netzwerke auch in Zukunft auf die in ihnen geteilten Inhalte angewiesen sein werden. Durch die Verwendung eines Social-Norm-Nudges zur Verringerung der Menge und des Empfängerkreises von persönlichen Daten wird zwangsläufig auch der Inhalt eines Netzwerkes reduziert. Darum ist es fragwürdig, ob ein Interesse sozialer Netzwerke am Einsatz entsprechender Nudges vorhanden ist. Doch der Vertrauensgewinn der Zielgruppe sowie die Tatsache, dass nicht jeder Inhalt persönliche Daten enthalten muss, könnten das Interesse der Betreiber von sozialen Netzwerken an einer Implementation dennoch wecken. Beispielsweise TikTok hat im Januar 2021 die Privatsphären-Optionen für Minderjährige verschärft und manche für gewisse Altersklassen standardmässig aktiviert (ByteDance Ltd., o. D.-a). Die Plattform verwendet somit den Default-Nudge, woran zu erkennen ist, dass ihren Betreibern der Schutz der Privatsphäre von Nutzenden zentral erscheint. Vielleicht orientiert sich die Konkurrenz in Zukunft an der Strategie von TikTok.

Auch eine Implementation über Drittanbieter wäre denkbar. Vor allem für Kinder und Jugendliche könnte eine solche Umsetzung sinnvoll sein, um ihnen den Umgang mit persönlichen Daten zu lehren. Es kann nicht angenommen werden, dass sich junge Personen unterdurchschnittlich stark um ihre Daten kümmern, denn in mehreren Studien wird ein vorhandenes Bewusstsein für den Umgang mit persönlichen Daten belegt (Bernath et al., 2020; Blank et al., 2014; Boyd & Hargittai, 2010; Kokolakis, 2017). Allerdings nahm seit 2012 der Anteil der Jugendlichen, die Einstellungen zum Schutz der Privatsphäre aktiviert haben ab. Daher könnte sich der Einsatz von Nudges auch bei Jugendlichen als nützlich erweisen.

Zusammenfassend konnten in dieser Bachelorarbeit mit einer experimentellen Umfrage neue Erkenntnisse erlangt werden. Nun liegt es an sozialen Netzwerken oder anderen potenziellen Anbietern, das Wissen zu vertiefen und Nudges zur Erhöhung des Schutzes der Privatsphäre in sozialen Netzwerken anzuwenden.

11 Literaturverzeichnis

- Abramova, O., Wagner, A., Krasnova, H. & Buxmann, P. (2017). Understanding Self-Disclosure on Social Networking Sites – A Literatur Review. *23rd America Conference on Information Systems*. Berlin, Deutschland: ResearchGate.
- Acquisti, A., John, L. K. & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research*, 49(2), 160–174. <https://doi.org/10.1509/jmr.09.0215>
- Altman, I. (1981). *The Environment and Social Behavior*. New York, Vereinigte Staaten: Wadsworth Publishing Company, Inc.
- Asch, S. E. (1955). Opinions and Social Pressure. *Scientific American*, 193(5), 31–35. <https://doi.org/10.1038/scientificamerican1155-31>
- Aschermann, T. (2019, 19. September). Wie funktioniert Instagram: Eine kleine Einführung. Abgerufen am 5. April 2021, von https://praxistipps.chip.de/wie-funktioniert-instagram-eine-kleine-einfuehrung_3508
- Ausprung, K., Hinz, T. & Liebig, S. (2009). Komplexität von Vignetten, Lerneffekte und Plausibilität im Faktoriellen Survey. *Methoden – Daten – Analysen*, 3(1), 59–96.
- Barak, A. & Gluck-Ofri, O. (2007). Degree and Reciprocity of Self-Disclosure in Online Forums. *CyberPsychology & Behavior*, 10(3), 407–417. <https://doi.org/10.1089/cpb.2006.9938>
- Bekker, P. (2016, 28. September). Was ist Twitter? Einfach erklärt. Abgerufen am 17. April 2021, von https://praxistipps.chip.de/was-ist-twitter-einfach-erklaert_49887
- Bernath, J., Suter, L., Waller, G., Külling, C., Willemse, I. & Süss, D. (2020). *JAMES – Jugend, Aktivitäten, Medien – Erhebung Schweiz*. Zürcher Hochschule für Angewandte Wissenschaften. Abgerufen von https://www.zhaw.ch/storage/psychologie/upload/forschung/medienpsychologie/james/2020/ZHAW_Bericht_JAMES_2020_de.pdf
- Betschon, S. (2018, 19. Dezember). Facebook-Skandale: Die neusten Enthüllungen. *Neue Zürcher Zeitung*. Abgerufen von <https://www.nzz.ch>
- Biesinger, R. (2018). Dopamin und das Belohnungssystem. In *Dopamin und das Belohnungssystem* (S. 63–71). https://doi.org/10.1007/978-3-658-23526-0_6

- Blank, G., Bolsover, G. & Dubois, E. (2014). A New Privacy Paradox: Young People and Privacy on Social Network Sites. *SSRN Electronic Journal*. Published. <https://doi.org/10.2139/ssrn.2479938>
- Boaz, D. (2021, 3. Juni). libertarianism. Abgerufen am 3. Juli 2021, von <https://www.britannica.com/topic/libertarianism-politics>
- Boyd, D. & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*. Published. <https://doi.org/10.5210/fm.v15i8.3086>
- Bundesamt für Gesundheit. (o. D.-a). Übergewicht und Adipositas. Abgerufen am 3. Juli 2021, von <https://www.bag.admin.ch/bag/de/home/gesund-leben/gesundheitsfoerderung-und-praevention/koerpergewicht/uebergewicht-und-adipositas.html>
- Bundesamt für Gesundheit. (o. D.-b). Zahlen & Fakten: Tabak. Abgerufen am 3. Juli 2021, von <https://www.bag.admin.ch/bag/de/home/zahlen-und-statistiken/zahlen-fakten-zu-sucht/zahlen-fakten-zu-tabak.html#:~:text=Im%20Jahr%202017%20rauchten%20in,den%20Frauen%2023%2C3%25>.
- Bundesamt für Statistik. (2018). Übergewicht. Abgerufen am 3. Juli 2021, von <https://www.bfs.admin.ch/bfs/de/home/statistiken/gesundheits/determinanten/uebergewicht.html>
- Bundesamt für Statistik. (o. D.-a). Bevölkerung. Abgerufen am 29. März 2021, von <https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/stand-entwicklung/bevoelkerung.html>
- Bundesamt für Statistik. (o. D.-b). Sprachen. Abgerufen am 29. März 2021, von <https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/sprachen-religionen/sprachen.html>
- ByteDance Ltd. (o. D.-a). Einstellungen zu Privatsphäre und Sicherheit für Nutzer*innen unter 18 Jahren | TikTok Hilfe-Center. Abgerufen am 5. April 2021, von <https://support.tiktok.com/de/account-and-privacy/account-privacy-settings/privacy-and-safety-settings-for-users-under-age-18>
- ByteDance Ltd. (o. D.-b). Einstellungen zur Privatsphäre | TikTok Hilfe-Center. Abgerufen am 5. April 2021, von <https://support.tiktok.com/de/account-and-privacy/account-privacy-settings/privacy-controls>
- Cambridge University. (o. D.). popularity. In *Cambridge Dictionary*. Abgerufen von <https://dictionary.cambridge.org/de/worterbuch/englisch/popularity>

- Chartrand, T. L. & Bargh, J. A. (1999). The chameleon effect: The perception–behavior link and social interaction. *Journal of Personality and Social Psychology*, 76(6), 893–910. <https://doi.org/10.1037/0022-3514.76.6.893>
- Cheung, C., Lee, Z. W. Y. & Chan, T. K. H. (2015). Self-disclosure in social networking sites. *Internet Research*, 25(2), 279–299. <https://doi.org/10.1108/intr-09-2013-0192>
- Christofides, E., Muise, A. & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, 12(3), 341–345. <https://doi.org/10.1089/cpb.2008.0226>
- Cialdini, R. B., Kallgren, C. A. & Reno, R. R. (1991). A Focus Theory of Normative Conduct: A Theoretical Refinement and Reevaluation of the Role of Norms in Human Behavior. *Advances in Experimental Social Psychology*, (24), 201–234. [https://doi.org/10.1016/s0065-2601\(08\)60330-5](https://doi.org/10.1016/s0065-2601(08)60330-5)
- Cozby, P. (1972). Self-Disclosure, Reciprocity and Liking. *Sociometry*, 35(1), 151. <https://doi.org/10.2307/2786555>
- Cozby, P. (1973). Self-disclosure: A literature review. *Psychological Bulletin*, 79(2), 73–91. <https://doi.org/10.1037/h0033950>
- Debatin, B., Lovejoy, J. P., Horn, A. K. & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108. <https://doi.org/10.1111/j.1083-6101.2009.01494.x>
- Díaz Ferreyra, N., Meis, R. & Heisel, M. (2017). Online Self-disclosure: From Users' Regrets to Instructional Awareness. *Lecture Notes in Computer Science*, 83–102. https://doi.org/10.1007/978-3-319-66808-6_7
- Drerup, J. & Voloj Dessauer, A. (2016). Von kleinen Stupsern und großen Schubsern – Politik und Ethik des Libertären Paternalismus auf dem Prüfstand. *Zeitschrift für Praktische Philosophie*, 3(1), 347–436. <https://doi.org/10.22613/zfpp/3.1.12>
- Dreßing, H., Bailer, J., Anders, A., Wagner, H. & Gallas, C. (2014). Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact Upon Victims. *Cyberpsychology, Behavior, and Social Networking*, 17(2), 61–67. <https://doi.org/10.1089/cyber.2012.0231>

- Dworkin, G. (1972). PATERNALISM. *The Monist*, 1(56), 64–84. Abgerufen von <http://www.jstor.org/stable/27902250>
- Facebook Inc. (2018, 30. November). Teilt Instagram Stories mit euren engen Freunden. Abgerufen am 5. April 2021, von <https://about.instagram.com/de-de/blog/announcements/curate-instagram-stories-for-close-friends-only>
- Facebook Inc. (2021, Januar). *FB Earnings Presentation Q4 2020*. Abgerufen von https://s21.q4cdn.com/399680738/files/doc_financials/2020/q4/FB-Earnings-Presentation-Q4-2020.pdf
- Facebook Inc. (o. D.-a). Aus welchen Zielgruppen kann ich auswählen, wenn ich Inhalte auf Facebook teile? Abgerufen am 5. April 2021, von https://www.facebook.com/help/211513702214269?helpref=faq_content
- Facebook Inc. (o. D.-b). Privatsphäre-Einstellungen und Informationen. Abgerufen am 5. April 2021, von <https://www.facebook.com/help/instagram/196883487377501>
- Falch, M., Henten, A., Tadayoni, R. & Windekilde, I. (2009). Business Models in Social Networking. *CMI International Conference*. Ballerup, Dänemark. Abgerufen von https://www.researchgate.net/publication/242178725_Business_Models_in_Social_Networking
- Figli, K. & Lehrer, C. (2020). Privacy Nudging: How the Design of Privacy Settings Affects Disclosure in Social Networks. *Research-in-Progress Papers*. Abgerufen von <https://research.cbs.dk/en/publications/privacy-nudging-how-the-design-of-privacy-settings-affects-disclo>
- Gerber, P., Volkamer, M. & Gerber, N. (2017). Das Privacy-Paradoxon – Ein Erklärungsversuch und Handlungsempfehlungen. *Dialogmarketing Perspektiven*, (2016/2017), 139–167. https://doi.org/10.1007/978-3-658-16835-3_8
- Golder, L., Jans, C., Venetz, A., Bohn, D. & Herzog, N. (2019, Mai). *Sexuelle Belästigung und sexuelle Gewalt an Frauen sind in der Schweiz verbreitet*. gfs.bern. Abgerufen von <https://cockpit.gfsbern.ch/de/cockpit/sexuelle-gewalt-in-der-schweiz/>
- Gonçalves, D., Coelho, P., Martinez, L. F. & Monteiro, P. (2021). Nudging Consumers toward Healthier Food Choices: A Field Study on the Effect of Social Norms. *Sustainability*, 13(4), 1660. <https://doi.org/10.3390/su13041660>

- Google LLC. (o. D.). Datenschutzeinstellungen für Videos ändern - Computer - YouTube-Hilfe. Abgerufen am 5. April 2021, von <https://support.google.com/youtube/answer/157177?co=GENIE.Platform%3DDesktop&hl=de#zippy=%2C%C3%B6ffentliche-videos%2Cprivate-videos%2Cnicht-gelistete-videos>
- Gregor, S. & Lee-Archer, B. (2016). The digital nudge in social security administration. *International Social Security Review*, 69(3–4), 63–83. <https://doi.org/10.1111/issr.12111>
- Hallam, C. & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217–227. <https://doi.org/10.1016/j.chb.2016.11.033>
- Hollenbaugh, E. & Ferris, A. (2014). Facebook self-disclosure: Examining the role of traits, social cohesion, and motives. *Computers in Human Behavior*, 30, 50–58. <https://doi.org/10.1016/j.chb.2013.07.055>
- Hughes-Roberts, T. (2013). Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour? *International Conference on Social Computing*, 909–912. New York, Vereinigte Staaten: Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/socialcom.2013.140>
- Kahneman, D. & Schmidt, T. (2016). *Schnelles Denken, langsames Denken*.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Krämer, N. C. & Haferkamp, N. (2011). Online Self-Presentation: Balancing Privacy Concerns and Impression Construction on Social Networking Sites. *Privacy Online*, 127–141. https://doi.org/10.1007/978-3-642-21521-6_10
- Krämer, N. C. & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, 31, 67–71. <https://doi.org/10.1016/j.copsyc.2019.08.003>
- Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, 25(2), 109–125. <https://doi.org/10.1057/jit.2010.6>
- Langer, M. (2018, 18. März). Riesiger Datenmissbrauch blamiert Facebook | NZZ. *Neue Zürcher Zeitung*. Abgerufen von <https://www.nzz.ch>

- Lee, Y. H., Hsiao, C., Weng, J. & Chen, Y. H. (2020). The impacts of relational capital on self-disclosure in virtual communities. *Information Technology & People*, 34(1), 228–249. <https://doi.org/10.1108/itp-11-2018-0541>
- LinkedIn Corporation. (o. D.-a). Sichtbarkeit geteilter Beiträge. Abgerufen am 5. April 2021, von <https://www.linkedin.com/help/linkedin/answer/431?lang=de>
- LinkedIn Corporation. (o. D.-b). Was Personen in Ihrem Profil sehen können ? Abgerufen am 5. April 2021, von <https://www.linkedin.com/help/linkedin/answer/77>
- Liu, Y., Gummadi, K. P., Krishnamurthy, B. & Mislove, A. (2011). Analyzing facebook privacy settings. In Association for Computing Machinery (Hrsg.), *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference - IMC '11*. New York, Vereinigte Staaten: ACM Press. <https://doi.org/10.1145/2068816.2068823>
- Lutz, C. & Strathoff, P. (2014). Privacy Concerns and Online Behavior Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses. *SSRN Electronic Journal*. Published. <https://doi.org/10.2139/ssrn.2425132>
- Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>
- Masaki, H., Shibata, K., Hoshino, S., Ishihama, T., Saito, N. & Yatani, K. (2020). Exploring Nudge Designs to Help Adolescent SNS Users Avoid Privacy and Safety Threats. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–11. Honolulu, Vereinigte Staaten. <https://doi.org/10.1145/3313831.3376666>
- Masur, P. K. & Scharkow, M. (2016). Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies. *Social Media + Society*, 2(1), 205630511663436. <https://doi.org/10.1177/2056305116634368>
- Mirsch, T., Lehrer, C. & Jung, R. (2018). Digital Nudging: Altering User Behavior in Digital Environments. In J. M. Leimeister & W. Brenner (Hrsg.), *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)* (S. 643–648). St.Gallen, Schweiz. Abgerufen von <https://www.alexandria.unisg.ch/250315/>
- Momsen, K. & Stoerk, T. (2014). From intention to action: Can nudges help consumers to choose renewable energy? *Energy Policy*, 74(C), 376–382. <https://doi.org/10.1016/J.ENPOL.2014.07.008>

- Morando, F., Iemma, R. & Raiteri, E. (2014). Privacy evaluation: what empirical research on users' valuation of personal data tells us. *Internet Policy Review*, 3(2). <https://doi.org/10.14763/2014.2.283>
- Ng, M. (2014). Consumer motivations to disclose information and participate in commercial activities on Facebook. *Journal of Global Scholars of Marketing Science*, 24(4), 365–383. <https://doi.org/10.1080/21639159.2014.949372>
- Niemann, J., Schenk, M., Teutsch, D., Wlach, K. & Allgeier, Y. (2012). Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen (Schriftenreihe Medienforschung der LfM). In A. Roßnagel, G. Reinmann, J. Niemann & M. Schenk (Hrsg.), *Quantitative Befragung von Jugendlichen und jungen Erwachsenen* (Bd. 71, S. 159–267). Berlin, Deutschland: VISTAS Verlag GmbH.
- Pinterest Inc. (o. D.). Datenschutz für dein Konto bearbeiten. Abgerufen am 23. April 2021, von <https://help.pinterest.com/de/article/edit-account-privacy>
- Predan-Hallabrin, B. (2019, 30. September). Was ist Pinterest? Verständlich erklärt. Abgerufen am 23. April 2021, von https://praxistipps.chip.de/was-ist-pinterest-verstaendlich-erklaert_44795
- Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1). <https://doi.org/10.5210/fm.v15i1.2775>
- Reynolds, B., Venkatanathan, J., Gonçalves, J. & Kostakos, V. (2011). Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. *Human-Computer Interaction – INTERACT 2011*, 204–215. Berlin, Heidelberg, Deutschland: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-23765-2_14
- Rudin, B. (2003). Privatheit im Internet? In G. Schwarz & K. Hummler (Hrsg.), *Das Recht auf sich selbst: Bedrohte Privatsphäre im Spannungsfeld zwischen Sicherheit und Freiheit*. (S. 137–147). Zürich, Schweiz: Verlag Neue Züricher Zeitung.
- Santor, D., Messervey, D. & Kusumakar, V. (2000). Measuring Peer Pressure, Popularity, and Conformity in Adolescent Boys and Girls: Predicting School Performance, Sexual Attitudes, and Substance Abuse. *Journal of Youth and Adolescence*, 29(2), 163–182. <https://doi.org/10.1023/a:1005152515264>

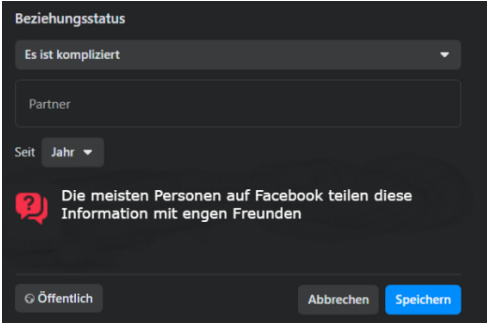
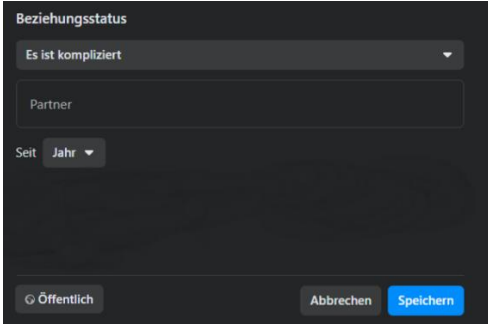
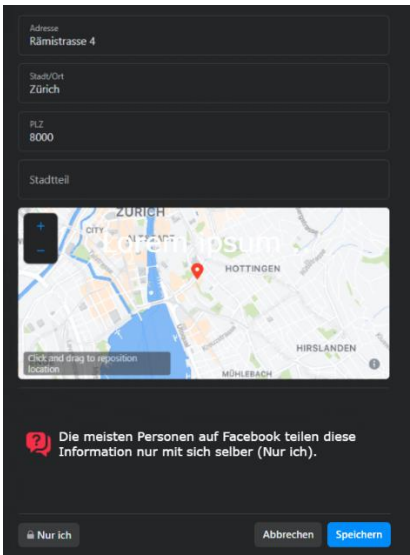
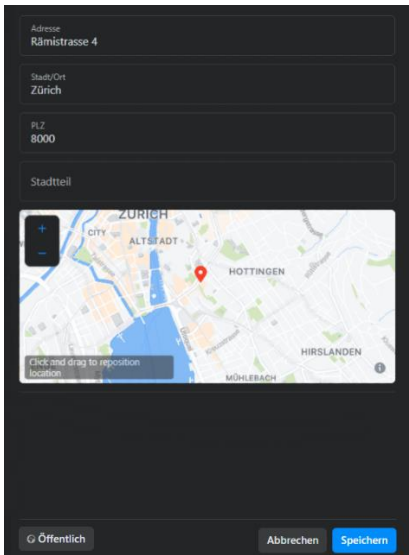

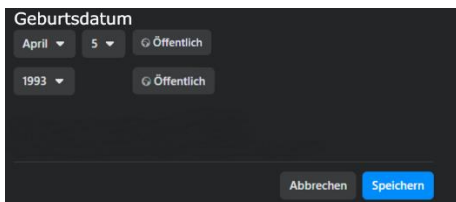

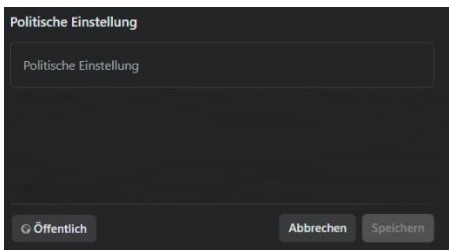
- Schär, A. & Stanoevska-Slabeva, K. (2019). *Application of Digital Nudging in Customer Journeys - A Systematic Literature Review*. Gehalten auf der Digital Nudging in Customer Journeys Twenty-fifth Americas Conference on Information Systems, Cancun, Mexico. Abgerufen von https://www.researchgate.net/publication/333149840_Application_of_Digital_Nudging_in_Customer_Journeys_-_A_Systematic_Literature_Review
- Schneider, J. (2019, 16. Juli). Was ist LinkedIn? Einfach erklärt. Abgerufen am 5. April 2021, von https://praxistipps.chip.de/was-ist-linkedin-einfach-erklart_41613
- Snap Inc. (o. D.). Datenschutzeinstellungen. Abgerufen am 5. April 2021, von <https://support.snapchat.com/de-DE/a/privacy-settings2>
- Stibe, A. & Cugelman, B. (2019). Social Influence Scale for Technology Design and Transformation. In D. Lamas, F. Loizides, L. Nacke, H. Petrie, M. Winckler & P. Zaphiris (Hrsg.), *Human-Computer Interaction – INTERACT 2019* (S. 561–577). Cham, Schweiz: Springer International Publishing. https://doi.org/10.1007/978-3-030-29387-1_33
- Stok, F. M. & de Ridder, D. T. D. (2019). The Focus Theory of Normative Conduct. In M. L. W. Vliek & K. Sassenberg (Hrsg.), *Social Psychology in Action* (S. 95–110). Cham, Schweiz: Springer. https://doi.org/10.1007/978-3-030-13788-5_7
- Sunstein, C. R. (2014). Nudging: A Very Short Guide. *Journal of Consumer Policy*, 37(4), 583–588. <https://doi.org/10.1007/s10603-014-9273-1>
- Sunstein, C. R. & Thaler, R. H. (2003). Libertarian Paternalism Is Not an Oxymoron. *The University of Chicago Law Review*, 70(4), 1159–1202. <https://doi.org/10.2307/1600573>
- SurveyMonkey. (o. D.-a). Konfidenzintervallrechner. Abgerufen am 12. Juli 2021, von <https://www.surveymonkey.de/mp/margin-of-error-calculator/>
- SurveyMonkey. (o. D.-b). Stichprobenrechner: Stichprobengrößen verstehen. Abgerufen am 13. Januar 2021, von <https://www.surveymonkey.de/mp/sample-size-calculator/>
- Taddicken, M. (2011). Selbstoffenbarung im Social Web. *Publizistik*, 56(3), 281–303. <https://doi.org/10.1007/s11616-011-0123-8>

- Taddicken, M. (2014). The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248–273. <https://doi.org/10.1111/jcc4.12052>
- Tamir, D. & Mitchell, J. (2012). Disclosing information about the self is intrinsically rewarding. *Proceedings of the National Academy of Sciences*, 109(21), 8038–8043. <https://doi.org/10.1073/pnas.1202129109>
- Taskin, S. (2015, 12. Juni). Was ist YouTube? Einfach erklärt. Abgerufen am 5. April 2021, von https://praxistipps.chip.de/was-ist-youtube-einfach-erklart_41471
- Thaler, R. H. & Sunstein, C. R. (2003). Libertarian Paternalism. *American Economic Review*, 93(2), 175–179. <https://doi.org/10.1257/000282803321947001>
- Thaler, R. H. & Sunstein, C. R. (2009). *Nudge: Wie man kluge Entscheidungen anstößt*. Berlin, Deutschland: Ullstein Buchverlage GmbH.
- Trepte, S. & Dienlin, T. (2015). Privatsphäre im Internet. In S. Pieschl & T. Porsch (Hrsg.), *Neue Medien und deren Schatten: Mediennutzung, Medienwirkung und Medienkompetenz* (1. Auflage 2014 Aufl., S. 53–80). <https://doi.org/10.1007/978-3-642-21521-6>
- Tufekci, Z. (2007). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28(1), 20–36. <https://doi.org/10.1177/0270467607311484>
- Twitter Inc. (o. D.-a). Informationen zur Auffindbarkeit über E-Mail und Telefonnummer. Abgerufen am 17. April 2021, von <https://help.twitter.com/de/safety-and-security/email-and-phone-discoverability-settings>
- Twitter Inc. (o. D.-b). Über öffentliche und geschützte Tweets. Abgerufen am 17. April 2021, von <https://help.twitter.com/de/safety-and-security/public-and-protected-tweets#video>
- Utz, S., Tanis, M. & Vermeulen, I. (2012). It Is All About Being Popular: The Effects of Need for Popularity on Social Network Site Use. *Cyberpsychology, Behavior, and Social Networking*, 15(1), 37–42. <https://doi.org/10.1089/cyber.2010.0651>
- We Are Social, Hootsuite & DataReportal. (2021, Februar). *DIGITAL 2021: SWITZERLAND*. Abgerufen von <https://datareportal.com/reports/digital-2021-switzerland>

- Weinmann, M., Schneider, C. & Brocke, J. V. (2016). Digital Nudging. *Business & Information Systems Engineering*, 58(6), 433–436. <https://doi.org/10.1007/s12599-016-0453-1>
- White, M. (2013). *The Manipulation of Choice: Ethics and Libertarian Paternalism* (2013. Aufl.). New York, Vereinigte Staaten: Palgrave Macmillan. <https://doi.org/10.1057/9781137313577>
- Willemse, I., Waller, G., Süss, D., Genner, S. & Huber, A.-L. (2012). *JAMES – Jugend, Aktivitäten, Medien – Erhebung Schweiz*. Zürcher Hochschule für Angewandte Wissenschaften, Zürich. Abgerufen von https://www.zhaw.ch/storage/psychologie/upload/forschung/medienpsychologie/james/2012/Ergebnisbericht_JAMES_2012.pdf
- Wölwer, F. (2018, 9. September). Facebook - was ist das? Einfach erklärt. Abgerufen am 5. April 2021, von https://praxistipps.chip.de/facebook-was-ist-das-einfach-erklaert_41486
- Young, A. L. & Quan-Haase, A. (2013). PRIVACY PROTECTION STRATEGIES ON FACEBOOK. *Information, Communication & Society*, 16(4), 479–500. <https://doi.org/10.1080/1369118x.2013.777757>

12 Anhang

12.1 Anhang I

Nudge vorhanden	Nudge nicht vorhanden
	
	
	
	

<p>Politische Einstellung</p> <p>Politische Einstellung</p> <p>Die meisten Personen auf Facebook teilen diese Information nur mit engen Freunden</p> <p>Öffentlich Abbrechen Speichern</p>	<p>Religiöse Ansichten</p> <p>Religiöse Ansichten</p> <p>Öffentlich Abbrechen Speichern</p>
<p>Sexuelle Orientierung</p> <p>Sexuelle Orientierung</p> <p>Die meisten Personen auf Facebook teilen diese Information nur mit engen Freunden.</p> <p>Öffentlich Abbrechen Speichern</p>	<p>Sexuelle Orientierung</p> <p>Sexuelle Orientierung</p> <p>Öffentlich Abbrechen Speichern</p>
<p>Alkohol</p> <p>Trinkst du Alkohol ?</p> <p>Die meisten Personen auf Facebook teilen diese Information nur mit Freunden.</p> <p>Öffentlich Abbrechen Speichern</p>	<p>Alkohol</p> <p>Trinkst du Alkohol ?</p> <p>Öffentlich Abbrechen Speichern</p>
<p>Krankheiten</p> <p>Krankheiten</p> <p>Die meisten Personen auf Facebook teilen diese Information mit sich selbst (Nur ich).</p> <p>Öffentlich Abbrechen Speichern</p>	<p>Krankheiten</p> <p>Krankheiten</p> <p>Öffentlich Abbrechen Speichern</p>
<p>Rauchen</p> <p>Rauchst du?</p> <p>Die meisten Personen auf Facebook teilen diese Information mit Freunden.</p> <p>Öffentlich Abbrechen Speichern</p>	<p>Rauchen</p> <p>Rauchst du?</p> <p>Öffentlich Abbrechen Speichern</p>
<p>martina.mustfrau@mustermail.ch</p> <p>Öffentlich</p> <p>Die meisten Personen auf Facebook teilen diese Information nur mit sich selbst (Nur Ich).</p> <p>Abbrechen Speichern</p>	<p>martina.mustfrau@mustermail.ch</p> <p>Öffentlich</p> <p>Abbrechen Speichern</p>

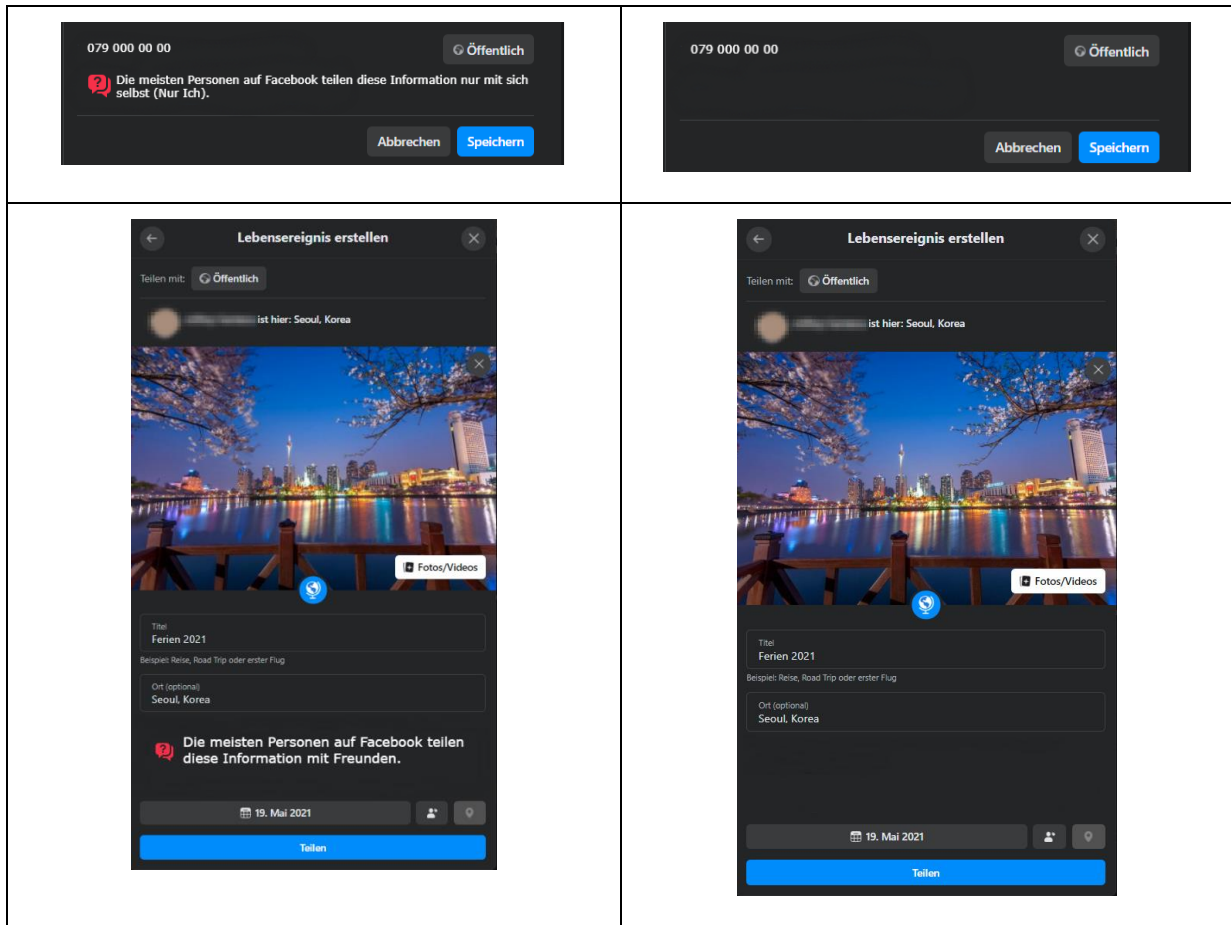


Tabelle 17: Vollständige Auflistung aller Nudges im Experiment.

Quelle: eigene Darstellung. Eingabemasken wurden von Facebook genommen und angepasst.

12.2 Anhang II

Variable	Frage	Skalenniveau	Ausprägungen (Codes)	Begründung	Hypothese
Social Norm Digital Nudge					
SNDN	{rand(1,2)}	nominal	1 "nicht vorhanden" 2 "vorhanden"	Automatisch ausgefüllt, Befragte sieht es nicht	H1, H2a, H3a, H4a
Soziale Netzwerke					
SN0	Wie oft benutzen Sie folgende soziale Netzwerke pro Woche?				
SN1	TikTok	ordinal	0 "Ich habe kein Account" 1 "seltener als einmal pro Woche" 2 "mehrmals in der Woche" 3 "mehrmals am Tag"	Nebensächlich	Informativ
SN2	Instagram				
SN3	Snapchat				
SN4	Facebook				
SN5	YouTube				
SN6	Pinterest				
SN7	Twitter				
SN8	LinkedIn				

Selbstoffenbarung					
ohne Nudge (SNDN1 = 2) (Verhalten Soziale Netzwerke 1)					
oSNDN1	Stellen Sie sich bitte vor, dass Sie auf Facebook einen neuen Account erstellen. Dort müssen Sie zwölf persönliche Informationen angeben. Sie sind gerade dabei, Ihr Geburtsdatum einzugeben. Nun müssen Sie auswählen, mit wem Sie Ihr Geburtsdatum teilen möchten. Welche Option würden Sie wählen?	ordinal	0 Nur ich 1 Enge Freunde 2 Freunde 3 Freunde von Freunden 4 Öffentlich	Experiment (angelehnt an Dimensionen von Díaz Ferreyra, Meis und Heisel (2017))	H1, H2a, H2b, H3a, H3b, H4a, H4b
oSNDN2	Nun kommen Sie zur nächsten Angabe. Sie sind nun dabei, ihren Beziehungsstatus einzugeben. Sie müssen auswählen, mit wem Sie Ihren Beziehungsstatus teilen möchten. Welche Option würden Sie wählen?				

oSNDN3	Sie sind nun dabei, auszuwählen, mit wem Sie die sexuelle Orientierung teilen möchten. Welche Option würden Sie wählen?				
oSNDN4	Sie sind nun dabei, auszuwählen, mit wem Sie die Religion, an die Sie glauben, teilen würden. Welche Option würden Sie wählen?				
oSNDN5	Sie sind nun dabei, auszuwählen, mit wem Sie die Partei, die Sie unterstützen, teilen würden. Welche Option würden Sie wählen?				
oSNDN6	Sie sind nun dabei, auszuwählen, mit wem Sie die Angabe teilen, ob und wie oft Sie Rauchen. Welche Option würden Sie wählen?				

oSNDN7	Sie sind nun dabei, auszuwählen, mit wem Sie die Angabe teilen, ob und wie oft Sie Alkohol trinken. Welche Option würden Sie wählen?				
oSNDN8	Sie sind nun dabei, auszuwählen, mit wem Sie die Krankheiten, die Sie haben teilen würden. Welche Option würden Sie wählen?				
oSNDN9	Sie sind nun dabei, auszuwählen, mit wem Sie die Adresse, wo Sie wohnen, teilen würden. Welche Option würden Sie wählen?				
oSNDN10	Sie sind nun dabei, auszuwählen, mit wem Sie die Orte, an denen Sie waren, teilen würden. Welche Option würden Sie wählen?				

oSNDN11	Sie sind nun dabei, auszuwählen, mit wem Sie ihre E-Mail-Adresse teilen würden. Welche Option würden Sie wählen?				
oSNDN12	Sie sind nun dabei, auszuwählen, mit wem Sie Ihre Telefonnummer teilen würden. Welche Option würden Sie wählen?				
mit Nudge (SNDN1 = 1) (Verhalten Soziale Netzwerke 2)					
mSNDN_1	Stellen Sie sich bitte vor, dass Sie auf Facebook einen neuen Account erstellen. Dort müssen Sie zwölf persönliche Informationen angeben. Sie sind gerade dabei, Ihr Geburtsdatum einzugeben. Nun müssen Sie auswählen, mit wem Sie Ihr Geburtsdatum teilen möchten.	ordinal	<ul style="list-style-type: none"> 0 Nur ich 1 Enge Freunde 2 Freunde 3 Freunde von Freunden 4 Öffentlich 	Experiment (angelehnt an Dimensionen von Díaz Ferreyra, Meis und Heisel (2017))	H1, H2a, H2b, H3a, H3b, H4a, H4b

	Welche Option würden Sie wählen?				
mSNDN_2	Nun kommen Sie zur nächsten Angabe. Sie sind nun dabei, ihren Beziehungsstatus einzugeben. Sie müssen auswählen, mit wem Sie Ihren Beziehungsstatus teilen möchten. Welche Option würden Sie wählen?				
mSNDN_3	Sie sind nun dabei, auszuwählen, mit wem Sie die sexuelle Orientierung teilen möchten. Welche Option würden Sie wählen?				
mSNDN_4	Sie sind nun dabei, auszuwählen, mit wem Sie die Religion, an die Sie glauben, teilen würden. Welche Option würden Sie wählen?				

mSNDN_5	Sie sind nun dabei, auszuwählen, mit wem Sie die Partei, die Sie unterstützen, teilen würden. Welche Option würden Sie wählen?				
mSNDN_6	Sie sind nun dabei, auszuwählen, mit wem Sie die Angabe teilen, ob und wie oft Sie Rauchen. Welche Option würden Sie wählen?				
mSNDN_7	Sie sind nun dabei, auszuwählen, mit wem Sie die Angabe teilen, ob und wie oft Sie Alkohol trinken. Welche Option würden Sie wählen?				
mSNDN_8	Sie sind nun dabei, auszuwählen, mit wem Sie die Krankheiten, die Sie haben teilen würden. Welche Option würden Sie wählen?				

mSNDN_9	Sie sind nun dabei, auszuwählen, mit wem Sie die Adresse, wo Sie wohnen, teilen würden. Welche Option würden Sie wählen?				
mSNDN_10	Sie sind nun dabei, auszuwählen, mit wem Sie die Orte, an denen Sie waren, teilen würden. Welche Option würden Sie wählen?				
mSNDN_11	Sie sind nun dabei, auszuwählen, mit wem Sie ihre E-Mail-Adresse teilen würden. Welche Option würden Sie wählen?				
mSNDN_12	Sie sind nun dabei, auszuwählen, mit wem Sie Ihre Telefonnummer teilen würden. Welche Option würden Sie wählen?				

Risikobewusstsein (Risiko und Privatsphäre)					
RBS0	Bewerten Sie die folgenden Aussagen.	ordinal			H2a, H2b
RBS01	Insgesamt sehe ich eine echte Gefährdung meiner Privatsphäre durch meine Präsenz auf sozialen Netzwerken.	ordinal	1 "trifft nicht zu" 2 "trifft eher nicht zu" 3 "teils/teils" 4 "trifft eher zu" 5 "trifft zu".	nach Krasnova, Spiekermann, Koroleva & Hildebrand, 2010; Malhotra, Kim & Agarwal, 2004; Taddicken, 2014	
RBS02	Ich befürchte, dass mir aufgrund meiner Präsenz auf sozialen Netzwerken etwas Schlimmes passieren könnte.				
RBS03	Ich fühle mich nicht sicher bei der Veröffentlichung meiner persönlichen Daten auf sozialen Netzwerken.				
RBS04	Ich bin besorgt über einen möglichen Online-Identitätsdiebstahl.				

RBS05	Ich bin besorgt darüber, dass sich meine Follower als jemand anders ausgeben.				
RBS06	Ich bin besorgt darüber, dass Personen, die ich nicht kenne, persönliche Informationen über mich sehen.				
RBS07	Insgesamt finde ich es riskant, meine persönlichen Daten auf sozialen Netzwerken zu veröffentlichen.				
RBS08	Bitte bewerten Sie, wie Sie das Risiko für Ihre Privatsphäre bei der Nutzung von Sozialen Netzwerken insgesamt einschätzen.	ordinal	1 "sehr sicher" 2 "sicher" 3 "teils/teils" 4 "riskant" 5 "sehr riskant".		
RBS09	Haben Sie jemals Erfahrungen mit Cyberstalking gehabt?	nominal	0 "nein" 1 "ja"	Nebensächlich	Informativ

RBS10	Hat jemand jemals persönliche Informationen von Ihnen veröffentlicht, ohne Sie darüber zu informieren?	nominal	0 "nein" 1 "ja"	Nebensächlich	Informativ
RBS11	Hat sich jemals jemand sich als Sie ausgegeben in einem Sozialen Netzwerk?	nominal	0 "nein" 1 "ja"	Nebensächlich	Informativ
RBS12	Wie viele Freunde/Followers haben Sie auf ...?			Nebensächlich	Informativ
RBS13	TikTok	nominal	0 "weiss ich nicht" 1 "weniger als 50" 2 "50–100" 3 "101–200" 4 "201–300" 5 "301–400" 6 "mehr als 400"		
RBS14	Instagram				
RBS15	Snapchat				
RBS16	Facebook				
RBS17	YouTube				
RBS18	Pinterest				
RBS19	Twitter				
RBS20	Linkedin				

Gruppenkonformität (Verhalten in Gruppen)					
	Bewerten Sie die folgenden Aussagen.			nach Stibe & Cugelman, 2019	H4a, H4b
GKN01	Ich vergleiche mich mit anderen Personen.	ordinal	1 "trifft nicht zu" 2 "trifft eher nicht zu" 3 "teils/teils" 4 "trifft eher zu" 5 "trifft zu"		
GKN02	Ich vergleiche häufig, wie es mir im Vergleich zu anderen Personen geht.				
GKN03	Ich bewerte meine Leistung im Vergleich zu anderen.				
GKN04	Ich ziehe es vor, das zu tun, was andere Personen normalerweise tun.				
GKN05	Ich ziehe es vor, so zu handeln, wie alle anderen handeln.				
GKN06	Ich befolge Verhaltensweisen, die Menschen typischerweise tun.				

Bedürfnis nach Popularität (Beliebtheit)					
	Bewerten Sie die folgenden Aussagen.				
BNP01	Ich habe schon Dinge getan, die ich sonst nicht mache, um mich beliebter zu machen.	ordinal	1 "trifft nicht zu" 2 "trifft eher nicht zu" 3 "teils/teils" 4 "trifft eher zu" 5 "trifft zu".	nach Santor, Messervey & Kusumakar, 2000	H3a, H3b
BNP02	Ich habe schon Freunde vernachlässigt aufgrund dessen, was andere denken könnten.				
BNP03	Ich mache fast alles, um nicht als Versager angesehen zu werden.				
BNP04	Es ist mir wichtig, dass andere denken, dass ich beliebt bin.				
BNP05	Manchmal verbringe ich Zeit mit Personen, nur weil diese beliebt sind.				
BNP06	Ich habe schon Sachen gekauft, nur weil sie im Trend waren.				

BNP07	Teilweise wechsle ich die Art, mich zu kleiden, um beliebter zu sein.				
BNP08	Ich bin schon mit jemandem befreundet gewesen, nur weil andere Personen diese Person mögen.				
BNP09	Ich bin schon auf Partys gegangen, nur um Teil der Menge zu sein.				
BNP10	Ich mache oft Dinge, nur um bei Menschen beliebt zu sein.				
BNP11	Manchmal bin ich mit Leuten unterwegs, damit andere nicht denken, ich sei unbeliebt.				
BNP12	Ich habe Angst, von anderen als unbeliebt wahrgenommen zu werden.				
KF01	Bitte wählen Sie die Zahl 4 aus				

Demografische Merkmale					
DM1	Geschlecht	nominal	0 "weiblich" 1 "männlich" 2 "divers"	Demographisch	Informativ
DM2	Alter	metrisch (intervall)	Alter	Demographisch	Informativ
DM3	Höchster Abschluss	nominal	0 "obligatorische Schule" 1 "Berufslehre" 2 "Berufsmaturität" 3 "gymnasiale Maturität oder Fachmaturität" 4 "Bachelor FH/Uni oder ETH" 5 "Master FH/Uni oder ETH" 6 "Eidg. Diplom /Fachausweis" 7 "Diplom höhere Fachschule"	Demographisch	Informativ
DM4	Erwerbstätigkeit	nominal	0 "Ich bin vollzeit-erwerbstätig" 1 "Ich bin teilzeit-erwerbstätig" 2 "Ich bin in Mutterschafts-/Erziehungsurlaub" oder in sonstiger Beurlaubung 3 Ich bin Auszubildende(r)/Lehrling/ Umschüler(in) 4 Ich bin zur Zeit nicht erwerbstätig (einschliesslich: Studenten, die nicht gegen Geld arbeiten, Arbeitslose, Vorruhestand, Rentner) 5 "Ich bin erwerbstätig und im Studium"	Demographisch	Informativ

Tabelle 18: Forscherversion des Fragebogens.

12.3 Anhang III

Dateiname	Beschreibung
Anhang III/Auswertung	
Auswertung_Bachelorarbeit.sps	Syntax der Bearbeitungen am Datensatz und der Auswertungen für die Bachelorarbeit.
Auswertung_Bachelorarbeit_H1_nach_Bildung.sps	Syntax der Auswertung der ersten Hypothese aufgeteilt nach Bildung
Auswertung_Bachelorarbeit_H1_nach_Erwerbstätigkeit.sps	Syntax der Auswertung der ersten Hypothese aufgeteilt nach Erwerbstätigkeit
Auswertung_Bachelorarbeit_H1_nach_Geschlecht.sps	Syntax der Auswertung der ersten Hypothese aufgeteilt nach Geschlecht.
Auswertung_Bachelorarbeit_mit_19_bis_24.sps	Syntax der Regression durchgeführt nur mit denjenigen, die sich in der Altersgruppe 19 bis 24 befinden.
Auswertung_Bachelorarbeit_ohne_19_bis_24.sps	Syntax aller Auswertungen wie in Auswertung_Bachelorarbeit.sps ohne die Altersgruppe 19 bis 24.
Anhang III / Daten	
daten_umfrage.sav	Importierte Daten aus der Umfrage ohne weitere Bearbeitung
daten_umfrage_nach_auswertung.sav	Datensatz mit umcodierten und neu codierten Variablen
daten_umfrage_nach_auswertung_nur_19_bis_24.sav	Datensatz nur mit Personen in der Altersgruppe 19 bis 24
daten_umfrage_nach_auswertung_ohne_19_bis_24.sav	Datensatz nur mit Personen die nicht in der Altersgruppe 19 bis 24 sind.
Anhang III / Daten	
survey_483831_SPSS_syntax_file.sps	Syntaxfile erstellt durch LimeSurvey für den Datenimport.

Bisher erschienene Schriften

Ergebnisse von Forschungsprojekten erscheinen jeweils in Form von Arbeitsberichten in Reihen.
Sonstige Publikationen erscheinen in Form von alleinstehenden Schriften.

Derzeit gibt es in den Churer Schriften zur Informationswissenschaft folgende Reihen:

Reihe Berufsmarktforschung

Weitere Publikationen

Churer Schriften zur Informationswissenschaft – Schrift 131

Herausgegeben von Wolfgang Semar

Patrik Jurkovic

Erfolgsgarant Lean-Startup Approach?

Chur, 2021

ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 132

Herausgegeben von Wolfgang Semar

Sandra Rumiz

Firmenarchive in Wikimedia-Projekten

Wie Bestände von Schweizer Textilunternehmen über Wikipedia und Wikidata auffindbar werden

Chur, 2021

ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 133

Herausgegeben von Wolfgang Semar

Vanessa Seyffert

Chatbots und Semantic-Web – ein "Dream-Team"?

Einsatz semantischer Technologien in der Chatbot-Entwicklung und

Anwendung im Bibliotheksbereich

Chur, 2021

ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 134

Herausgegeben von Wolfgang Semar

Mircea Obreja

Loss Aversion im E-Commerce

Moderierende Faktoren bezüglich des digitalen Loss Aversion Nudges

in der Purchase-Stage

Chur, 2021

ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 135

Herausgegeben von Wolfgang Semar

Vanessa Brogli

Messinstrumente für die Untersuchung der Lesekompetenz

Wie sich Effekte auf das Lesen bei Leseförderung von Bibliotheken untersuchen lassen

Chur, 2021

ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 136

Herausgegeben von Wolfgang Semar

Nichola Schwendimann

Cloud Readiness von Schweizer IT-KMU

Untersucht anhand von zwei Mikrounternehmen

Chur, 2021

ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 137

Herausgegeben von Wolfgang Semar

Stefanie Moser

Homeoffice für Bibliotheksmitarbeitende von öffentlichen und wissenschaftlichen Bibliotheken

in der Schweiz während der COVID-19-Pandemie

Chur, 2021

ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 138
Herausgegeben von Wolfgang Semar
Mara Funaro
Ursachen für die geringe Verbreitung von Extreme Programming
Weshalb sich lediglich Praktiken der agilen Methode durchgesetzt haben
Chur, 2021
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 139
Herausgegeben von Wolfgang Semar
Debora Messerli
Nachhaltigkeitsprojekte in Bibliotheken
Massnahmenkatalog zur Vermittlung der UN-Agenda 2030 in Öffentlichen und Wissenschaftlichen
Bibliotheken
Chur, 2021
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 140
Herausgegeben von Wolfgang Semar
Noemi Andres
Status quo des Social-Media-Einsatzes in Schweizer Tambouren-, Clairon- und Pfeifervereinen
Chur, 2021
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 141
Herausgegeben von Wolfgang Semar
Rachel Noëmi Thommen
Lärmmanagement an Deutschschweizer Hochschulbibliotheken
Evaluation der Wahrnehmung des Geräuschpegels von Studierenden in Hochschulbibliotheken
und Einfluss von Covid-19
Chur, 2021
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 142
Herausgegeben von Wolfgang Semar
Daria Gloor
Berichterstattung von CO₂-Emissionen im Scope 3 des GHG Protocol
Eine Fallstudie zur Ableitung von digitalen Best Practices für Unternehmen zur Messung
und Angabe von CO₂-Emissionen der Kriterien im Scope 3
Chur, 2022
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 143
Herausgegeben von Wolfgang Semar
Leonardo Personini
What role have academic libraries and librarians had in the fight against the COVID-19 pandemic?
Chur, 2022
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 144
Herausgegeben von Wolfgang Semar
Jasmin Suter
TikTok User sind einfacher manipulierbar
Einfluss von Videoplattformen auf das Verhalten in der Pre-Purchase Phase am Beispiel TikTok
Chur, 2022
ISSN 1660-945X

Churer Schriften zur Informationswissenschaft – Schrift 145
Herausgegeben von Wolfgang Semar
Lea Bächli
Die Veränderungen der Angebote öffentlicher Bibliotheken in der Deutschschweiz durch die
COVID-19-Pandemie
Chur, 2022
ISSN 1660-945X

Über die Informationswissenschaft der Fachhochschule Graubünden

Die Informationswissenschaft ist in der Schweiz noch ein relativ junger Lehr- und Forschungsbereich. International weist diese Disziplin aber vor allem im anglo-amerikanischen Bereich eine jahrzehntelange Tradition auf. Die klassischen Bezeichnungen dort sind Information Science, Library Science oder Information Studies. Die Grundfragestellung der Informationswissenschaft liegt in der Betrachtung der Rolle und des Umgangs mit Information in allen ihren Ausprägungen und Medien sowohl in Wirtschaft und Gesellschaft. Die Informationswissenschaft wird in Chur integriert betrachtet.

Diese Sicht umfasst nicht nur die Teildisziplinen Bibliothekswissenschaft, Archivwissenschaft und Dokumentationswissenschaft. Auch neue Entwicklungen im Bereich Medienwirtschaft, Informations- und Wissensmanagement und Big Data werden gezielt aufgegriffen und im Lehr- und Forschungsprogramm berücksichtigt.

Der Studiengang Informationswissenschaft wird seit 1998 als Vollzeitstudiengang in Chur angeboten und seit 2002 als Teilzeit-Studiengang in Zürich. Seit 2010 rundet der Master of Science in Business Administration das Lehrangebot ab.

Der Arbeitsbereich Informationswissenschaft vereinigt Cluster von Forschungs-, Entwicklungs- und Dienstleistungspotenzialen in unterschiedlichen Kompetenzzentren:

- Information Management & Competitive Intelligence
- Collaborative Knowledge Management
- Information and Data Management
- Records Management
- Library Consulting
- Information Laboratory
- Digital Education

Diese Kompetenzzentren werden im Swiss Institute for Information Science (SII) zusammengefasst.

Impressum

Impressum

FHGR - Fachhochschule
Graubünden
Information Science
Pulvermühlestrasse 57
CH-7000 Chur

www.informationsscience.ch

www.fhgr.ch

ISSN 1660-945X

Institutsleitung

Prof. Dr. Ingo Barkow

Telefon: +41 81 286 24 61

Email: ingo.barkow@fhgr.ch

Sekretariat

Telefon: +41 81 286 24 24

Fax: +41 81 286 24 00

Email: clarita.decurtins@fhgr.ch